Texas International Law Journal

Volume 50 | Spring & Summer 2015 | Numbers 2 & 3

Volume 50, Issues 2 & 3

The University of Texas School of Law

TEXAS
INTERNATIONAL
LAW
JOURNAL

Volume 50
Numbers 2 & 3
Spring & Summer 2015

CONTENTS

SYMPOSIUM ISSUE 2

ARTICLES

NOTES

TEXAS
INTERNATIONAL
LAW
JOURNAL

Volume 50
Numbers 2 & 3
Spring & Summer 2015

CONTENTS

ISSUE 3

ARTICLES

NOTES

In the rapidly expanding discipline of international law, the *Texas International Law Journal* helps readers stay abreast and informed of recent developments and new scholarship by providing access to leading international legal, theoretical, and policy analysis. The *Journal* publishes academic articles, essays, and student notes in the areas of public and private international law, international legal theory, the law of international organizations, comparative and foreign law, and domestic laws with significant international implications. The editors and staff aim to fulfill these needs by concentrating on groundbreaking articles that will be useful to both practitioners and scholars. We hope you enjoy this latest issue.

The *Journal* is among the oldest and best-established student-published international law journals in the United States. In the wake of the Bay of Pigs disaster and the Cuban Missile Crisis, our publication began as an offshoot of the Texas International Law Society.[1] In January 1965, under the guidance of Professor E. Ernest Goldstein, we planted the Texas flag in the international arena with our first issue, entitled *The Journal of the University of Texas International Law Society*. Publications thereafter were biannual, taking the name *Texas International Law Forum* until summer 1971, when the *Journal* adopted its present title and began publishing three or four issues per year. Of the more than one hundred student-published international law journals across the country, only three schools have an older international heritage: Harvard, Columbia, and Virginia.

Over the years, the *Journal* staff has made the most of its established heritage. We have developed international repute by forging close ties with numerous scholars and authors worldwide. As a result, we receive over six hundred unsolicited manuscripts each year and are extremely selective in our publication choices. This position has helped us develop one of the largest student-published subscription circulations of any international law journal in the United States. The *Journal*'s subscription base includes law schools, government entities, law firms, corporations, embassies, international organizations, and individuals from virtually every state in the U.S. and more than forty-five countries.

With over thirty editorial board members and more than eighty staff members made up of full-time J.D. and LL.M. students, the *Journal* maintains a refined and well-organized editing process. As economic integration accelerates and nations forge closer ties in the new millennium, we are confident the *Journal* will continue to provide a significant contribution to the burgeoning field of international law.

DISTINGUISHED AUTHORS

The *Journal* has been fortunate to publish articles from a number of eminent scholars, including:

The Honorable William O. Douglas, former Justice of the Supreme Court of the United States; **W. Page Keeton**, former dean of the University of Texas School of Law; **Thomas Buergenthal**, former president of the Inter-American Court of Human Rights; **Charles Alan Wright**, former professor at the University of Texas School of Law, co-author of the leading treatise *Federal Practice and Procedure*, and former president of the American Law Institute; **Louis Henkin**, former president of the American Society of International Law, chief reporter of the Restatement of Foreign Relations Law of the

1. E. Ernest Goldstein, *Thank You Fidel! Or How the International Law Society and the* Texas International Law Journal *Were Born*, 30 TEX. INT'L L.J. 223 (1995).

United States, and former editor-in-chief of the *American Journal of International Law*; **the Honorable Richard J. Goldstone**, member of the Constitutional Court of South Africa and former chief prosecutor of the United Nations International War Crimes Tribunal for the former Yugoslavia and Rwanda; and **the Honorable Dalia Dorner**, Associate Justice of the Supreme Court of Israel.

OUTSTANDING CONTRIBUTORS

Our submissions consistently reflect the highest degree of quality from outstanding professionals, including:

Robert Reich, former U.S. Secretary of Labor, former professor of government and public policy at Harvard University, and former director of public policy for the Federal Trade Commission; **Joseph Jove**, former U.S. ambassador to Mexico; **Andreas Lowenfeld**, professor at New York University School of Law and leading international law scholar; **Dean Rusk**, U.S. Secretary of State under President Johnson; **Ewell "Pat" Murphy**, former chairman of the International Law Section of the American Bar Association and respected practicing attorney in the field of international business transactions; **Walter S. Surrey**, former chairman of the National Council for U.S.-China Trade and former president of the American Society of International Law; and **W. Michael Reisman**, professor at Yale Law School and member the board of directors of the American Society of International Law.

MISSION STATEMENT

Practitioners, scholars, and courts of all levels have cited articles from the *Texas International Law Journal* as legal authority since its first issue appeared in 1965. Members of the *Journal* seek to maintain this tradition of excellence for our 44th continuous year of publishing by providing the legal community with the highest quality of secondary source material on current and relevant international legal developments.

COPYRIGHT

The *Texas International Law Journal* (ISSN 0163-7479) is published three or four times a year by University of Texas School of Law Publications.

Cite as: TEX. INT'L L.J.

SUBSCRIPTIONS

Annual subscriptions to the *Journal* are available at the following rates:

$45.00 for domestic subscribers
$40.00 for *TILJ* alumni and current law students
$50.00 for foreign subscribers

To subscribe to the *Texas International Law Journal*, order reprints, or indicate a change of address, please visit www.tilj.org or write to:

University of Texas School of Law Publications
P.O. Box 8670
Austin, TX 78713
www.TexasLawPublications.com

Subscriptions are renewed automatically unless timely notice of termination is received. For any questions or problems concerning a subscription, please contact our Business Manager at (512) 232-1149 or Publications@law.utexas.edu.

BACK ISSUES

William S. Hein & Co., Inc. holds the back stock rights to all previous volumes of the *Texas International Law Journal.* For back issues and previous volumes of the *Journal*, please direct inquiries to:

William S. Hein & Co., Inc.
1285 Main St.
Buffalo, NY 14209
www.wshein.com

THE *FORUM*

The *Texas International Law Journal Forum* is the online companion to our printed volumes. The *Forum* publishes original scholarship on topics relating to recent developments in international law, as well as responses to scholarship printed in the *Texas International Law Journal.*

As with the *Journal*, all submissions are reviewed blindly throughout the year on a rolling basis. For more information regarding the *Forum*, please contact our Managing Editors at tilj@law.utexas.edu or visit www.tilj.org/forum.

ANNUAL SYMPOSIUM

The *Journal* hosts an annual symposium offering in-depth treatment of a topic of international legal concern. The purpose of these symposia is to promote the awareness of important developments in the formation of international law and to forge closer ties among scholars, practitioners, students, and members of the global legal community. We welcome your interest in these events. For more information regarding our annual symposium, please contact our Symposium Coordinator at tilj@law.utexas.edu or visit www.tilj.org/symposium.

MANUSCRIPT SUBMISSIONS AND EDITORIAL POLICIES

In conformity with the standard practice of scholarly legal publications in the United States, the *Texas International Law Journal* holds copyrights to its published works. Neither the Editorial Board nor the University of Texas are in any way responsible for the views expressed by contributors.

The *Journal* welcomes submissions from scholars, practitioners, businesspeople, government officials, and judges on topics relating to recent developments in international law. In addition to articles, the *Journal* also invites authors to submit shorter works, such as comments, book reviews, essays, notes, and bibliographies. All submissions are reviewed blindly throughout the year on a rolling basis.

We accept both hard-copy and electronic submissions. Please send article submissions, accompanied by a curriculum vitae, cover letter, and abstract, to the attention of the Submissions Editor. Manuscripts should conform with *The Bluebook: A Uniform System of Citation* (Columbia Law Review Ass'n et al. eds., 18th ed. 2005) and, to the extent feasible, follow *The Chicago Manual of Style* (Univ. of Chicago Press, 15th ed. 2003). Manuscripts should be typewritten and footnoted where necessary.

All submission inquiries and requests for review should be directed to the Submissions Editor at:

Submissions Editor
Texas International Law Journal
The University of Texas School of Law
727 E. Dean Keeton St.
Austin, TX 78705

Tel: (512) 232-1277
Fax: (512) 471-4299
E-Mail: tilj@law.utexas.edu
www.tilj.org

Jenna Al-Walawi
Brittney Angelich*
Paige Armstrong-Gutierrez*
Sara Block
Daniel Bradley*
Shelisa Brock*+
Alexander Brown
James Burnett*
Margaret Canell
Kristina Chung*+
Andrew Deas*
Marc-Anthony Delgado
Francesca Di Troia*
Michael Duran
David Fawcett
Lindsay Forbes*
Leslie Gardner
Leah Glowacki*
Todd Hartis*
Christopher Hefner
Lindsey Henrikson*
JC Hernandez
Blake Jenkins*
Brittany Johnson*
Sandra Jonas*
Navneet Khinda
Travis Korman
Brendan Lally-McGurl
Jessica Lance*
Craig Lauchner
Sung Hwan Lee
Grace Lentz
Katy Leung
Bobby Levinski*
Cesar Leyva*
Huayang Ma^
Cody Martinez
Nina-Belle Mbayu
Sean McClay
Natalie McDermon*+
Adam Nelson*
Michael Nelson*
Pamela Nickell
Cameron Njaa*
Ashley Nwonuma
Simone Otenaike*
Jade Peterkin
Kristin Petkova
Joseph Piorkowski*
James Quail
Tyler Richardson
Julia Rubio*
Peter Rush
Hayden Schottlaender*
Adelaide Schwartz
Joanna Serrato*
Ayomide Shittu*+
Vidushi Shrimali
Sara Siegel
Maxwelle Sokol*
Victoria Stephen*
Patrick Tatum*
Julie Thompson*
Stephen Villarreal*
Meghan Wied*
Anna Ziemnicki
Bryan Zubay

* Third-Year Member + LL.M. Member ^ Abroad/Away

THE UNIVERSITY OF TEXAS SCHOOL OF LAW

ADMINISTRATIVE OFFICERS

WARD FARNSWORTH, B.A., J.D.; *Dean, John Jeffers Research Chair in Law.*
JOHN B. BECKWORTH, B.A., J.D.; *Associate Dean for Administrtion and Strategic Planning, Lecturer.*
ROBERT M. CHESNEY, B.S., J.D.; *Associate Dean for Academic Affairs, Charles I. Professor in Law.*
WILLIAM E. FORBATH, A.B., B.A., Ph.D., J.D.; *Associate Dean for Research, Lloyd M. Bentsen Chair in Law.*
EDENE E. HARRINGTON, J.D.; *Associate Dean for Experiential Education., Dirictor of William Wayne Justice Center for Public Interest Law.*
MARIA M. ARRELLAGA, B.S.; *Assistant Dean for Communication.*
ELIZABETH T. BANGS, A.B., J.D.; ASSISTANT DEAN FOR STUDENT AFFAIRS.
KIMBERLY L. BIAR, B.B.A.; *Assistant Dean for Financial Affairs, Certified Public Accountant.*
MICHAEL G. HARVEY; *Assistant Dean for Technology.*
MONICA K. INGRAM, B.A., J.D.; *Assistant Dean for Admissions and Financial Aid.*
TIMOTHY A. KUBATZKY, B.A.; *Executive Director of Development.*
DAVID A. MONTOYA, B.A., J.D.; *Assistant Dean for Career Services.*
GREGORY J. SMITH, B.A., J.D.; *Assistant Dean for Continuing Legal Education.*

FACULTY EMERITI

HANS W. BAADE, A.B., J.D., LL.B., LL.M.; *Hugh Lamar Stone Chair Emeritus in Civil Law.*
RICHARD V. BARNDT, B.S.L., LL.B.; *PROFESSOR EMERITUS.*
JULIUS G. GETMAN, B.A., LL.B, LL.M.; *Earl E. Sheffield Regents Chair Emeritus.*
WILLIAM W. GIBSON, JR., B.A., LL.B.; *Sylvan Lang Professor Emeritus in Law of Trusts.*
ROBERT W. HAMILTON, A.B., J.D.; *Minerva House Drysdale Regents Chair Emeritus.*
DOUGLAS LAYCOCK, B.A., J.D.; *Alice McKean Young Regents Chair Emeritus.*
J. L. LEBOWITZ, A.B., J.D., LL.M.; *Joseph C. Hutcheson Professor Emeritus.*
BASIL F. MARKESINIS, LL.B., Ph.D., D.C.L., LL.D.; *JAMAIL REGENTS CHAIR EMERITUS IN LAW.*
JOHN T. RATLIFF, JR., B.A., LL.B.; *Ben Gardner Sewell Professor Emeritus in Civil Trial Advocacy.*
JAMES M. TREECE, B.A., J.D., M.A.; *Charles I. Francis Professor Emeritus in Law.*

PROFESSORS

JEFFREY B. ABRAMSON, B.A., J.D., Ph.D.; *Professor of Law and Government.*
DAVID E. ADELMAN, B.A., Ph.D., J.D.; *Harry Reasoner Regents Chair in Law.*
DAVID A. ANDERSON, A.B., J.D.; *Fred and Emily Marshall Wulff Centennial Chair in Law.*
MARK L. ASCHER, B.A., M.A., J.D., LL.M.; *Joseph D. Jamail Centennial Chair in Law.*
RONEN AVRAHAM, M.B.A., LL.B., LL.M., S.J.D.; *Thomas Shelton Maxey Professor in Law.*
MARILYN ARMOUR, B.A., M.S.W., Ph.D.; *Associate Professor*
LYNN A. BAKER, B.A., B.A., J.D.; *Frederick M. Baron Chair in Law, Co-Director of Center on Lawyers, Civil Justice, and the Media.*
MITCHELL N. BERMAN, A.B., M.A., J.D.; *Richard Dale Endowed Chair in Law, Professor of Philosophy, Co-Director of Law and Philosophy Program.*
BARBARA A. BINTLIFF, M.A., J.D.; *Joseph C. Hutcheson Professor in Law, Director of Tarlton Law Library and the Jamail Center for Legal Research.*
LYNN E. BLAIS, A.B., J.D.; *Leroy G. Denman, Jr. Regents Professor in Real Property Law.*
ROBERT G. BONE, B.A., J.D.; *G. Rollie White Teaching Excellence Chair in Law.*
OREN BRACHA, LL.B., S.J.D.; *Howrey LLP and Arnold, White, & Durkee Centennial Professor.*
DANIEL M. BRINKS, A.B., J.D., Ph.D; *Associate Professor and Co-Director of Bernard and Audre Rapoport Center for Human Rights and Justice.*
J. BUDZISZEWSKI, B.A., M.A., Ph.D.; *Professor.*
NORMA V. CANTU, B.A., J.D.; *Professor of Law and Education.*
LOFTUS C. CARSON, II, B.S., M. Pub. Aff., M.B.A., J.D.; *Ronald D. Krist Professor.*
MICHAEL J. CHURGIN, A.B., J.D.; *Raybourne Thompson Centennial Professor.*
JANE M. COHEN, B.A., J.D.; *Edward Clark Centennial Professor.*
FRANK B. CROSS, B.A., J.D.; *Herbert D. Kelleher Centennial Professor of Business Law.*
WILLIAM H. CUNNINGHAM, B.A., M.B.A., Ph.D.; *James L. Bayless Chair for Free Enterprise.*
JENS C. DAMMANN, J.D., LL.M., Dr. Jur., J.S.D.; *William Stamps Farish Professor in Law.*
JOHN DEIGH, B.A., M.A., Ph.D.; *Professor of Law and Philosophy.*
MECHELE DICKERSON, B.A., J.D.; *Arthur L. Moller Chair in Bankruptcy Law and Practice.*
GEORGE E. DIX, B.A., J.D.; *George R. Killam, Jr. Chair of Criminal Law.*
JOHN S. DZIENKOWSKI, B.B.A., J.D.; *Dean John F. Sutton, Jr. Chair in Lawyering and the Legal Process.*
KAREN L. ENGLE, B.A., J.D.; *Cecil D. Redford Prof. in Law, Director of Bernard & Audre Rapoport Center for Human Rights & Justice.*
KENNETH FLAMM, Ph.D.; *Professor.*
MIRA GANOR, B.A., M.B.A., LL.B., LL.M., J.S.D.; *Professor.*
JULIUS G. GETMAN, B.A., LL.B., LL.M.; *Earl E. Sheffield Regents Chair.*
CHARLES E. GHOLZ, B.S., B.S., Ph.D., *Associate Professor.*
JOHN M. GOLDEN, A.B., J.D., Ph.D.; *Loomer Family Professor in Law.*
STEVEN GOODE, B.A., J.D.; *W. James Kronzer Chair in Trial and Appellate Advocacy, University Distinguished Teaching Professor.*
LINO A. GRAGLIA, B.A., LL.B.; *A. Dalton Cross Professor.*
BENJAMIN G. GREGG, B.A., Ph.D; *Professor.*
CHARLES G. GROAT, B.A., M.S., Ph.D.; *Professor.*
PATRICIA I. HANSEN, A.B., M.P.A., J.D.; *J. Waddy Bullion Professor.*
HENRY T. HU, B.S., M.A., J.D.; *Allan Shivers Chair in the Law of Banking and Finance.*
BOBBY R. INMAN, B.A.; Lyndon B. *Johnson Centennial Chair in National Policy.*

DEREK P. JINKS, B.A., M.A., J.D.; *The Marrs McLean Professor in Law.*
STANLEY M. JOHANSON, B.S., LL.B., LL.M.; *James A. Elkins Centennial Chair in Law, University Distinguished Teaching Professor.*
CALVIN H. JOHNSON, B.A., J.D.; *Andrews & Kurth Centennial Professor.*
SUSAN R. KLEIN, B.A., J.D.; *Alice McKean Young Regents Chair in Law.*
JENNIFER E. LAURIN, B.A., J.D.; *Professor.*
SANFORD V. LEVINSON, A.B., Ph.D., J.D.; *W. St. John Garwood & W. St. John Garwood, Jr. Centennial Chair in Law, Professor of Gov't.*
ANGELA K. LITTWIN, B.A., J.D.; *Professor.*
VIJAY MAHAJAN, M.S.Ch.E., Ph.D.; *John P. Harbin Centennial Chair in Business.*
INGA MARKOVITS, LL.M.; *"The Friends of Joe Jamail" Regents Chair.*
RICHARD S.MARKOVITS, B.A., LL.B., Ph.D.; *John B. Connally Chair.*
THOMAS O.MCGARITY, B.A., J.D.; *Joe R. and Teresa Lozano Long Endowed Chair in Administrative Law.*
STEVEN A.MOORE, B.A., Ph.D.; *Bartlett Cocke Regents Professor in Architecture.*
LINDA S.MULLENIX, B.A., M. Phil., J.D., Ph.D.; *Morris & Rita Atlas Chair in Advocacy.*
STEVEN P. NICHOLS, B.S.M.E., M.S.M.E., J.D., Ph.D.; *Clint W. Murchison, Sr. Fellow of Free Enterprise.*
ROBERT J. PERONI, B.S.C., J.D., LL.M.; *The Fondren Foundation Centennial Chair for Faculty Excellence.*
H. W. PERRY, JR., B.A., M.A., Ph.D.; *Associate Professor of Law and Government.*
LUCAS A. POWE, JR., B.A., J.D.; *Anne Green Regents Chair in Law, Professor of Government.*
WILLIAM C. POWERS, JR., B.A., J.D.; *Hines H. Baker and Thelma Kelley Baker Chair, University Distinguished Teaching Professor.*
DAVID M. RABBAN, B.A., J.D.; *Dahr Jamail, Randall Hage Jamail, & Robert Lee Jamail Reg. Chair, Univ. Distinguished Teaching Prof.*
ALAN S. RAU, B.A., LL.B.; *Mark G. and Judy G. Yudof Chair in Law.*
DAVID W. ROBERTSON, B.A., LL.B., LL.M., J.S.D.; *W. Page Keeton Chair in Tort Law, University Distinguished Teaching Professor.*
JOHN A. ROBERTSON, A.B., J.D.; *Vinson & Elkins Chair.*
MARY ROSE, A.B., M.A., Ph.D.; *Associate Professor.*
WILLIAM M. SAGE, A.B., M.D., J.D.; *Vice Provost for Health Affairs, James R. Dougherty Chair for Faculty Excellence.*
LAWRENCE G. SAGER, B.A., LL.B.; *Alice Jane Drysdale Sheffield Regents Chair.*
JOHN J. SAMPSON, B.B.A., LL.B.; *William Benjamin Wynne Professor.*
CHARLES M. SILVER, B.A., M.A., J.D.; *Roy W. and Eugenia C. MacDonald Endowed Chair in Civil Procedure, Professor of Government, Co-Director of Center on Lawyers, Civil Justice, and the Media.*
ERNEST E. SMITH, B.A., LL.B.; *Rex G. Baker Centennial Chair in Natural Resources Law.*
DAVID B. SPENCE, B.A., J.D., M.A., J.D.; *Professor of Business, Government and Society, and Law.*
JAMES C. SPINDLER, B.A., J.D.; *The Sylvan Lang Professor.*
JANE STAPLETON, B.S., Ph.D., LL.B., D.C.L., D.Phil.; *Ernest E. Smith Professor.*
JORDAN M. STEIKER, B.A., J.D.; *Judge Robert M. Parker Endowed Chair in Law.*
MICHAEL F. STURLEY, B.A., J.D.; *Fannie Coplin Regents Chair.*
JEFFREY K. TULIS, B.A., M.A., Ph.D.; *Associate Professor.*
GREGORY J. VINCENT, B.A., J.D., Ed.D.; *Professor.*
SRIRAM VISHWANATH, B.S., M.S., Ph.D.; *Associate Professor.*
WENDY E.WAGNER, B.A., M.E.S., J.D.; *Joe A. Worsham Centennial Professor.*
LOUISE WEINBERG, A.B., J.D., LL.M.; *William B. Bates Chair for the Administration of Justice.*
OLIN G.WELLBORN, A.B., J.D.; *William C. Liedtke, Sr. Professor.*
JAY L.WESTBROOK, B.A., J.D.; *Benno C. Schmidt Chair of Business Law.*
ABRAHAM L.WICKELGREN, A.B., Ph.D., J.D.; *Bernard J. Ward Professor in Law.*
SEAN H. WILLIAMS, B.A., J.D., *Professor.*
ZIPPORAH B.WISEMAN, B.A., M.A., LL.B.; *Thos. H. Law Centennial Professor in Law.*
PATRICK WOOLLEY, A.B., J.D.; *Beck, Redden & Secrest Professor in Law.*

ASSISTANT PROFESSORS

JOSEPH R. FISHKIN, B.A., M.Phil., D.Phil., J.D.
CARY C. FRANKLIN, B.A., M.S.T., D.Phil., J.D.
JAMES MCCLELLAND, B.S., Ph.D.
SUSAN C. MORSE, A.B., J.D.
TIMOTHY WERNER, B.A., M.A., Ph.D.

SENIOR LECTURERS, WRITING LECTURERS, AND CLINICAL PROFESSORS

ALEXANDRA W. *Albright, B.A., J.D.; Senior Lecturer.*
WILLIAM P. ALLISON, B.A., J.D.; *Clinical Prof., Director of Criminal Defense Clinic.*
WILLIAM H. BEARDALL, JR., B.A., J.D.; *Adjunct Professor, Director of Transnational Worker Rights Clinic.*
NATALIA V. BLINKOVA, B.A., M.A., J.D.; *Lecturer*
PHILLIP C. BOBBITT, A.B., J.D., Ph.D.; *Distinguished Sr. Lecturer.*
HUGH L. BRADY, B.A., J.D.; *Adjunct Professor, Director of Legislative Lawyering Clinic.*
KAMELA S. BRIDGES, B.A., B.J., J.D.; *Lecturer.*
JOHN C. BUTLER, B.B.A., Ph.D. *Clinical Professor.*
MARY R. CROUTER, A.B., J.D.; *Lecturer, Assistant Director of William Wayne Justice Center for Public Interest law.*
MICHELE Y. DEITCH, B.A., M.S., J.D.; *Senior Lecturer.*
TIFFANY J. DOWLING, B.A., J.D.; *Clinical Instructor, Director of Actual Innocence Clinic.*
LORI K. DUKE, B.A., J.D.; *Clinical Professor.*
ARIEL E. DULITZKY, J.D., LL.M.; *Clinical Professor, Director of Human Rights Clinic.*
ELANA S. EINHORN, B.A., J.D.; *Lecturer.*
TINA V. FERNANDEZ, A.B., J.D.; *Lecturer, Director of Pro Bono Program.*
LINDA FROST, B.A., M.ED., J.D, PH.D; *Clinical Associate Professor.*
DENISE L. GILMAN, B.A., J.D.; *Clinical Prof., Co-Director Immigration Clinic.*
BARBARA HINES, B.A., J.D.; *Clinical Professor, Co-Director Immigration Clinic.*
HARRISON KELLER, B.A., M.A., Ph.D.; *Vice Provost for Higher Education Policy, Senior Lecturer.*

BRIAN R. LENDECKY, B.B.A., M.P.A; *Senior Lecturer.*
JEANA A. LUNGWITZ, B.A., J.D.; *Clinical Professor, Director of Domestic Violence Clinic.*
TRACY W.MCCORMACK, B.A., J.D.; *Lecturer, Director of Advocacy Programs.*
F. SCOTT MCCOWN, B.S., J.D.; *Clinical Professor, Director of Children's Rights Clinic.*
ROBIN B.MEYER, B.A., M.A., J.D.; *Lecturer.*
RANJANA NATARAJAN, B.A., J.D.; *Clinical Professor, Director of Civil Rights Clinic.*
JANE A. O'CONNELL, B.A., M.S., J.D.; *Lecturer, Associate Director for Patron Services, Instruction, and Research.*
SEAN J. PETRIE, B.A., J.D.; *Lecturer.*
RACHAEL RAWLINS, B.A., M.R.P., J.D.; *Senior Lecturer.*
WAYNE SCHIESS, B.A., J.D.; *Senior Lecturer, Director of David J. Beck Center for Legal Research, Writing and Appellate Advocacy.*
RAOUL D. SCHONEMANN, B.A., LL.M., J.D.; *Clinical Professor.*
STACY ROGERS SHARP, B.S., J.D.; *Lecturer.*
PAMELA J. SIGMAN, B.A., J.D.; *Lecturer, Director Juvenile Justice Clinic.*
DAVID S. SOKOLOW, B.A., M.A., J.D., M.B.A.; *Distinguished Senior Lecturer, Director of Student Life.*
LESLIE L. STRAUCH, B.A., J.D.; *Clinical Professor.*
GRETCHEN S. SWEEN, B.A., M.A., Ph.D., J.D.; *Lecturer.*
MELINDA E. TAYLOR, B.A., J.D.; *Senior Lecturer, Director of Center for Global Energy, International Arbitration and Environmental Law.*
HEATHER K. WAY, B.A., B.J., J.D.; *Lecturer, Director of Community Development Clinic.*
ELIZABETH M. YOUNGDALE, B.A., M.L.I.S., J.D.; *Lecturer.*

ADJUNCT PROFESSORS AND OTHER LECTURERS

ELIZABETH AEBERSOLD, B.A., M.S.
WILLIAM R. ALLENSWORTH, B.A., J.D.
ANDREW W. AUSTIN, B.A., M.PHIL, J.D.
MARJORIE I. BACHMAN, B.S., J.D.
CRAIG D. BALL, B.A., J.D.
SHARON C. BAXTER, B.S., J.D.
KARL O. BAYER, B.A., M.S., J.D.
JERRY A. BELL, B.A., J.D.
ALLISON H. BENESCH, B.A., M.S.W., J.D.
CRAIG R. BENNETT, B.S., J.D.
JAMES B. BENNETT, B.B.A., J.D.
MURFF F. BLEDSOE, B.A., J.D.
WILLIAM P. BOWERS, B.B.A., J.D., LL.M.
STACY L. BRAININ, B.A., J.D.
ANTHONY W. BROWN, B.A., J.D.
JAMES E. BROWN, LL.B. PETER
TOMMY L. BROYLES, B.A., J.D.
W. AMON BURTON, JR., B.A., M.A., LL.B.
DAVID J. CAMPBELL, B.A., J.D.
AGNES E. CASAS, B.A., J.D.
RUBEN V. CASTANEDA, B.A., J.D.
EDWARD A. CAVAZOS, B.A., J.D.
LINDA BRAY CHANOW, B.A., J.D.
JEFF CIVINS, A.B., M.S., J.D.
ELIZABETH COHEN, B.A., M.S.W., J.D.
JAMES W. COLLINS, B.S., J.D.
PATRICIA J. CUMMINGS, B.A., J.D.
KEITH B. DAVIS, B.S., J.D.
SCOTT D. DEATHERAGE, B.A., J.D.
DICK DEGUERIN, B.A., LL.B.
ADAM R. DELL, B.A., J.D.
MELONIE M. DEROSE, B.A., J.D.
RICHARD D. DEUTSCH, B.A., J.D.
STEVEN K. DEWOLF, B.A., J.D.
REBECCA H. DIFFEN, B.A., J.D.
ANDREW S. DREIER, B.A., LL.M., J.D.
CASEY D. DUNCAN, B.A., M.L.I.S., J.D. JUDGE
PHILIP DURST, B.A., M.A., J.D., Ph.D.
JAY D. ELLWANGER, B.A., J.D.
EDWARD Z. FAIR, B.A., M.S.W., J.D.
JOHN C. FLEMING, B.A., J.D.
KYLE K. FOX, B.A., J.D.
DAVID C. FREDERICK, B.A., Ph.D., J.D.
GREGORY D. FREED, B.A., J.D.
FRED J. FUCHS, B.A., J.D.
RYAN M. GARCIA, B.G.S., J.D.
GRETTA GARDNER, B.A., J.D.
MICHAEL S. GOLDBERG, B.A., J.D.
MICHAEL J. GOLDEN, A.B., J.D.
DAVID M. GONZALEZ, B.A., J.D.
JOHN F. GREENMAN, B.A., M.F.A., J.D.
DAVID HALPERN, B.A., J.D.
ELIZABETH HALUSKA-RAUSCH, B.A., M.A., M.S., Ph.D.
KELLY L. HARAGAN, B.A., J.D.
CLINT A. HARBOUR, B.A., J.D., LL.M.
ROBERT L. HARGETT, B.B.A., J.D.
MARY L. HARRELL, B.A., J.D.
CHRISTOPHER S. HARRISON, Ph.D., J.D.
WILLIAM M. HART, B.A., J.D.
JOHN R. HAYS, JR., B.A., J.D.
SUSAN J. HIGHTOWER, B.A., M.A., J.D.
KENNETH E. HOUP, JR., J.D.
RANDY R. HOWRY, B.J., J.D.
MONTY G. HUMBLE, B.A., J.D.
JENNIFER D. JASPER, B.S., M.A., J.D.
DIRK M. JORDAN, B.A., J.D.
JEFFREY R. JURY, B.A., J.D.
PATRICK O. KEEL, B.A., J.D.
DOUGLAS L. KEENE, Ph.D.
CHARI L. KELLY, B.A., J.D.
JEAN A. KELLY, B.A., J.D.
ROBERT N. KEPPLE, B.A., J.D.
PAUL S. KIMBOL, B.A., J.D.
MARK L. KINCAID, B.B.A., J.D.
ALICE L. KING, B.A., J.D.
MICHAEL KRAZSENEK, B.S., J.D.
AMI L. LARSON, B.A., J.D.
JODI R. LAZAR, B.A., J.D.
KEVIN L. LEAHY, B.A., J.D.
DAVID P. LEIN, B.A., M.P.A., J.D.
ANDRES J. LINETZKY, LL.M.
JAMES LLOYD LOFTIS, B.B.A., J.D.
MANUEL LOPEZ, A.B., J.D.
MARIO LOYOLA, B.A., J.D.
ANDREW F.MACRAE, B.J., J.D.
JIM MARCUS, B.A., J.D.
HARY S. MARTIN, A.B., M.L.S., J.D.
FRANCES L.MARTINEZ, B.A., J.D.
LORI R. MASON, B.A., J.D.
PHILIP MAXWELL, B.A., J.D.
PETER C. MCCABE, B.A., J.D.
ANN M. MCGEEHAN, B.A., J.D.
BARRY F. MCNEIL, B.A., J.D.
MARGARET M. MENICUCCI, B.A., J.D.
JO ANN MERICA, B.A., J.D.
RANELLE M.MERONEY, B.A., J.D.
ELIZABETH N.MILLER, B.A., J.D.
JOHNATHAN F. MITCHELL, B.A., J.D.
DARYL L.MOORE, B.A., M.L.A., J.D.
EDWIN G.MORRIS, B.S., J.D.
JAMES C. MORRISS III, B.S., J.D.
SARAH J. MUNSON, B.A., J.D.
HENRY C. MYERS, B.S., J.D.
JOHN A. NEAL, B.A., J.D.
MANUEL H. NEWBURGER, B.A., J.D.

DAVID G. NIX, B.S.E., LL.M., J.D.
HOWARD D. NIRKEN, B.A., M.P.AFF., J.D.
CHRISTINE S. NICHIMARA, B.A., J.D.
PATRICK L. O'DANIEL, B.B.A., J.D.
M. ARIEL PAYAN, B.A., J.D.
MARK L. PERLMUTTER, B.S., J.D.
ELIZA T. PLATTS-MILLS, B.A., J.D.
JONATHAN PRATTER, B.A., M.L.S., J.D.
VELVA L. PRICE, B.A., J.D.
MARGARET K. REIN, B.A., J.D.
CLARK W. RICHARDS, B.A., LL.M., J.D.
BRIAN C. RIDER, B.A., J.D.
ROBERT M. ROACH, JR., B.A., J.D.
BRIAN J. ROARK, B.A., J.D.
BETTY E. RODRIGUEZ, B.S.W., J.D.
JAMES D. ROWE, B.A., J.D.
MATTHEW C. RYAN, B.A., J.D.
KAREN R. SAGE, B.A., J.D.
MARK A. SANTOS, B.A., J.D.
JAMES J. SCHESKE, B.A., J.D.
MICHAEL J. SCHLESS, B.A., J.D.
SUSA SCHULTZ, B.S., J.D.
AMY J. SCHUMACHER, B.A., J.D.
SUZANNE SCHWARTZ, B.J., J.D.
RICHARD J. SEGUAR, JR., B.A., J.D.
DAVID A. SHEPPARD, B.A., J.D.
JUDGE ERIC M. SHEPPERD, B.A., J.D.
ARTHUR H. SHERMAN, B.B.A., J.D.
RONALD J. SIEVERT, B.A., J.D.
AMBROSIO A. SILVA, B.S., J.D.
BEA A. SMITH, B.A., M.A., J.D.
LYDIA N. SOLIZ, B.B.A., J.D.
STEPHEN M. SOMENBERG, A.B., M.D.
JAMES M. SPELLINGS, B.S., J.D.
KACIE L. STARR, B.A., J.D.
WILLIAM F. STUTTS, B.A., J.D.
MATTHEW J. SULLIVAN, B.S., J.D.
GRETCHEN S. SWEEN, B.A., M.A., Ph.D., J.D.
BRADLEY P. TEMPLE, B.A., J.D.
SHERINE E. THOMAS, B.A., J.D.
TERRY O. TOTTENHAM, B.S., LL.M., J.D.
CARLOS R. TREVNIO, M.B.A., LL.M., J.D.
MICHAL S. TRUESDALE, B.A., M.A., J.D.
TIMOTHY J. TYLER, B.A., J.D.
SUSAN S. VANCE, B.B.A., J.D.
LANA K. VARNEY, B.J., J.D.
DEBORAH M.WAGNER, B.A., M.A., J.D.
CHRISTOPHER M. WEIMER, B.A., J.D.
WARE V.WENDELL, A.B., J.D.
RODERICK E. WETSEL, B.A., J.D.
THEA WHALEN, B.A., J.D.
DARA J.WHITEHEAD, B.A., M.S.
RANDALL B.WILHITE, B.B.A., J.D.
TIMOTHY A. WILKINS, A.B., M.D.
DAVID G.WILLE, B.S.E.E., M.S.E.E., J.D.
.ANDREW M. WILLIAMS, B.A., J.D.
CHRISTINA T. WISDOM, B.A., J.D.
TRAVIS M. WOHLERS, B.S., Ph.D., J.D.
LUCILLE D.WOOD, B.A., J.D.
DENNY L. WRIGHT, B.B.M, LL.M., J.D.
DANIEL J. YOUNG, B.A., J.D.
EVAN A. YOUNG, B.A., A.B., B.A., J.D.
TREVOR YOUNG, B.A., M.A., LL.M, J.D.

VISITING PROFESSORS

OWEN L. ANDERSON, B.A., J.D.
ANTONIO H. BENJAMIN, LL.B., LL.M.
VICTOR FERRERES, J.D., LL.M., J.S.D.
ALON KLEMENT, LL.B., B.A., LL.M., S.J.D.
GRAHAM B. STRONG, B.A., J.D., LL.M.

The Decline of International Humanitarian Law *Opinio Juris* and the Law of Cyber Warfare

MICHAEL N. SCHMITT* AND SEAN WATTS**

SUMMARY

* Charles H. Stockton Professor of International Law and Director, Stockton Center for the Study of International Law, United States Naval War College; Professor of Public International Law, Exeter University; Senior Fellow, NATO Cooperative Cyber Defence Centre of Excellence; Fellow, Harvard Law School Program on International Law and Armed Conflict. The views expressed are those of the author in his personal capacity.

** Professor, Creighton University School of Law, Omaha, Nebraska; Senior Fellow, Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia; Reserve Instructor, Department of Law, United States Military Academy at West Point, West Point, New York.

INTRODUCTION

International Humanitarian Law (IHL) has developed largely through a pluralistic process.[1] Its earliest codifications were inspired in no small part by religious and moral thinking.[2] Secular academic writers soon joined the process, making central contributions that are still cited as authoritative centuries later.[3] All the while, States published and refined military manuals and articles of war to instruct their armed forces in rules for the conduct of warfare.[4] By the late nineteenth century, States began to codify accepted expressions of IHL that accounted broadly for military custom, as well as notions of humanity, in a budding corpus of positive international law.[5] The compounded horrors of new weapons and industrial-scale battlefields fueled this and further codification.[6] While the twentieth century saw treaties take pride of place among IHL sources, customary international law, judgments of military and international tribunals, military legal doctrine, and humanitarian and academic commentary also helped to shape the content and evolution of IHL.[7]

Pluralism, however useful at accounting for diverse interests, has not come without cost. Despite prolonged attention and development, IHL exhibits a high degree of ambiguity. Few legal disciplines rival the indeterminacy of IHL. As Sir Hersch Lauterpacht, then Whewell Professor of International Law at the University of Cambridge and later judge on the International Court of Justice, famously observed, "if international law is, in some ways, at the vanishing point of law, the law of war is, perhaps even more conspicuously, at the vanishing point of international law."[8] Confronted with a cacophony of inputs—private and public, military and

---

1. LESLIE GREEN, THE CONTEMPORARY LAW OF ARMED CONFLICT 26–64 (3d ed. 2008); Christopher Greenwood, *Historical Development and Legal Basis*, *in* THE HANDBOOK OF INTERNATIONAL HUMANITARIAN LAW 1, 15–35 (Dieter Fleck ed., 2d ed. 2008); *see generally* GEOFFREY BEST, HUMANITY IN WARFARE (1980).

2. *See generally* G.I.A.D. Draper, *The Interaction of Christianity and Chivalry in the Historical Development of the Law of War*, 5 INT'L REV. RED CROSS 3 (1965).

3. *See generally* M. H. KEEN, THE LAWS OF WAR IN THE LATE MIDDLE AGES (Michael Hurst ed., 1965).

4. The paradigmatic example is the Lieber Code approved by President Lincoln for use by the Union Army during the U.S. Civil War. Instructions for the Government of Armies of the United States in the Field, General Orders No. 100, Apr. 24, 1863, *reprinted in* THE LAWS OF ARMED CONFLICTS 3 (Dietrich Schindler & Jiri Toman eds., 2004); Rick Beard, *The Lieber Codes*, N.Y. TIMES (Apr. 24, 2013), http:// opinionator.blogs.nytimes.com/2013/04/24/the-lieber-codes/.

5. *E.g.*, Geneva Convention for the Amelioration of the Condition of the Wounded in Armies in the Field, Aug. 22, 1864, 22 Stat. 940, 129 Consol. T.S. 361; The Hague Convention (II) with Respect to the Laws and Customs of War on Land and Its Annex: Regulations Respecting the Laws and Customs of War on Land, July 29, 1899, 32 Stat. 1803, 187 Consol. T.S. 429.

6. This dynamic was represented most notably by the work of Henri Dunant. *See* PIERRE BOISSIER, HISTORY OF THE INTERNATIONAL COMMITTEE OF THE RED CROSS: FROM SOLFERINO TO TSUSHIMA 19–25 (1985) (describing the gruesome aftermath of the Battle of Solferino that Dunant described in a book that was to inspire the creation of the International Red Cross).

7. *See generally* GEOFFREY BEST, WAR AND LAW SINCE 1945 (1994).

8. Hersch Lauterpacht, *The Problem of the Revision of the Law of War*, 29 BRIT. Y.B. INT'L L. 360, 382 (1952).

civilian, domestic and international—the IHL lawyer frequently finds clarity and consensus elusive. Sorting IHL noise from notes requires considerable legal, military, and political experience. The content and operation of even cardinal IHL principles such as distinction remain subject to voluble debate.

While a measure of its indeterminacy is surely attributable to IHL's pluralistic process of development, an equal measure must be traced to the unique and peculiar purpose of IHL. IHL is a body of law that countenances intentional killing and deprivation of liberty on a grand scale in pursuit of national interests, which may not be benign. It expressly allows for the deaths of innocents and destruction of their property to achieve military aims, while imposing obligations and requiring precautions that can expose combatants to tangibly greater danger. Yet, IHL also humanizes bloody battlefields. When respected, it can save lives and ensure humane treatment, preserving a degree of humanity in both the victims and victors of war.

In light of these competing dynamics, the interpretation and development of IHL must be handled delicately. A highly reactive body of law, IHL has seen evolutionary and even revolutionary changes instituted by States following armed conflicts—the classic example being adoption of the four Geneva Conventions in the aftermath of the Second World War.[9] Those with the expertise and experience to fully appreciate the fragile IHL balance between military necessity and humanity that provides its foundational *raison d'etre* have been the key drivers of this process of change.[10] Historically, States, and their military representatives in particular, have played this critical role in shaping the contours of IHL. To be sure, proposals by academics and non-governmental organizations have fostered significant enhancements of IHL. But this has occurred only after deliberate and studied consideration and acceptance by government experts and States uniquely positioned to evaluate the operational and even strategic costs of legal innovation. The result was an IHL reasonably assured to reflect the best achievable balance of military necessity and humanity—an IHL at once acceptable to the States and armed forces charged with its implementation and to the advocates for war's inevitable victims.

While the IHL dialogue remains vigorous, continuation of its pluralistic nature appears in doubt. In particular, a void of State participation, especially with respect to *opinio juris*, has formed. One no longer finds regular State expressions of IHL *opinio juris*. Nor does one regularly find comprehensive and considered responses by States to the proposals and pronouncements of non-State IHL participants. In many respects, as this article will demonstrate, the guns of State IHL *opinio juris* have fallen silent.

---

9. Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, Aug. 12, 1949, 6 U.S.T. 3114, 75 U.N.T.S. 31 (entered into force Oct. 21, 1950) [hereinafter GC I]; Geneva Convention for the Amelioration of the Condition of the Wounded, Sick and Shipwrecked Members of Armed Forces at Sea, Aug. 12, 1949, 6 U.S.T. 3217, 75 U.N.T.S. 85 (entered into force Oct. 21, 1950) [hereinafter GC II]; Geneva Convention Relative to the Treatment of Prisoners of War, Aug. 12, 1949, 6 U.S.T. 3316, 75 U.N.T.S. 135 (entered into force Oct. 21, 1950) [hereinafter GC III]; Geneva Convention Relative to the Protection of Civilian Persons in Time of War, Aug. 12, 1949, 6 U.S.T. 3516, 75 U.N.T.S. 287 (entered into force Oct. 21, 1950) [hereinafter GC IV].

10. *See* Michael N. Schmitt, *Military Necessity and Humanity in International Humanitarian Law: Preserving the Delicate Balance*, 50 VA. J. INT'L L. 795, 806–22 (2010) [hereinafter Schmitt, *Military Necessity*] (describing the discourse among States and military leaders, humanitarian NGOs, and nascent international courts and tribunals in shaping IHL's response to military necessity concerns).

Meanwhile, non-State IHL actors have been undeterred, even emboldened. The IHL contributions of the international legal academy have been particularly voluminous. Some are of exceptional quality. However, academia has also incentivized the production of decidedly unconventional IHL perspectives. While useful to illustrate or deconstruct normative architecture, many such efforts not only eschew rigorous legal analysis, but also display insensitivity to the realities of battle in favor of interpretive creativity or innovation. Indeed, many authors and pundits boldly masquerade legal innovations as accepted understandings of IHL.[11] Even more troubling is the fact that many scholars lacking the appropriate education or experiential background have responded to the fact that IHL is a topic *au courant* by claiming IHL expert status. Their work product misstates basic principles and rules with distressing frequency, and they are too often set forth in an ad hominem manner. All of these contributions, from the superb to the sub-standard, exert informal but real pressure on the shape of IHL.

Further complicating the IHL process, while helping to drown out what little State *opinio juris* one finds today, are the burgeoning efforts of humanitarian advocacy groups. These organizations and their members have long performed the valuable role of counterweight, urging States not to lead the law unduly askew in the pursuit of narrow national interests. Yet, assertions of law by humanitarian groups must be considered with some degree of care as their work in explicating IHL understandably (and often appropriately) reflects the legal causes and policies of their constituencies. Additionally, where they stand with respect to IHL depends on where they sit; what they observe and conclude about the battlefield and its law is always a function of their perceived mandates. Humanitarian activists working exclusively to alleviate the suffering of civilians and other protected persons will inevitably appreciate IHL differently than, for instance, soldiers charged with winning a battle or State policy-makers responsible for leading a nation to victory.

Other non-State entities also indirectly, but effectively, shape IHL. Foremost among these is the International Committee of the Red Cross (ICRC). The ICRC is undoubtedly the most influential single body in the field; indeed, few organizations or States field the IHL expertise or experience of its impressive Legal Division. However, in assessing issues arising from the military necessity-humanity balance, the ICRC unsurprisingly (and again often appropriately) tends to resolve grey areas in favor of humanitarian considerations, much as militaries usually do vis-à-vis military necessity. The United Nations Human Rights Council has also now included IHL matters within its portfolio. Although the Council's efforts have sometimes reflected a misunderstanding of IHL and inappropriately conflated IHL and human rights law,[12] more recent work has proved quite sophisticated and well measured.[13]

---

11. Of particular note is the IHL blogosphere that has recently materialized. It serves to conveniently highlight emerging issues and provides a first glimpse of IHL analysis. However, bloggers are frequently unable to offer the depth or expertise called for by complex IHL issues.

12. *See, e.g.*, Human Rights Council, *Human Rights in Palestine and Other Occupied Arab Territories: Rep. of the U.N. Fact-Finding Mission on the Gaza Conflict*, para. 284, U.N. Doc. A/HRC/12/48 (Sept. 25, 2009) [hereinafter *Goldstone Report*] ("A convergence between human rights protections and humanitarian law protections is also in operation. The rules contained in Article 75 of Additional Protocol I (AP I), which reflect customary law, define a series of fundamental guarantees and protections, such as the prohibitions against torture, murder and inhuman conditions of detention, recognized also under human rights law.").

And, of course, the growing number of international tribunals—standing, ad hoc, and bifurcated—that also pronounce on the scope and meaning of IHL, often in confounding prolixity, must be added to this complex admixture of non-State influences on IHL content and vector.

In the face of these and other influences, it is essential to recall that States, *and only States*, "make" IHL.[14] They alone enjoy legal competency to interpret international law beyond the confines of a particular case. States do so either through treaty or through "general practice accepted as law," the latter component known as customary international law.[15] As will be explained, expressions of *opinio juris* operate as the fulcrum around which new customary humanitarian law norms crystallize, as well as a basis for the contextual interpretation and development of existing treaty and customary IHL principles and rules.

Expressions of *opinio juris* are a tool by which States regulate the emergence, interpretation, and evolution of legal norms. Effectively employed, they may maximize achievement and protection of States' perceived national interests. By failing regularly to offer such expressions, States risk unintended Grotian Moments, that is, "radical developments in which new rules and doctrines of customary international law emerge with unusual rapidity and acceptance."[16] Such episodes do not necessarily create "bad" law, nor do they always run contrary to States' interests or intentions, but they often represent brief periods when States' ability to reason objectively is at its nadir. They are therefore a suboptimal time for States to engage in activities that amount to norm formation and development.

This article sets forth thoughts regarding the performance of States, particularly the United States, in this informal process of meta-norm formation and evolution. Although the topic of the symposium from which the article emanated was the law of cyber warfare, the discussion is decidedly non-cyber in nature. It is intentionally so, as the objective is to identify recent tendencies in the process that might foreshadow how IHL governing cyber operations is likely to develop absent a reversal of current trends. Our examination suggests that non-State actors are outpacing and, in some cases displacing, State action in both quantitative and qualitative terms. States seem reticent to offer expressions of *opinio juris*, often for good reasons. We argue that such reticence comes at a cost—diminished influence on the content and application

---

13. *See generally* Human Rights Council, *Rep. of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism*, U.N. Doc. A/HRC/25/59 (Mar. 10, 2014) (by Ben Emmerson) [hereinafter *Emmerson Report*]; Human Rights Council, *Rep. of the Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions*, U.N. Doc. A/HRC/23/47 (Apr. 9, 2013) (by Christof Heyns) [hereinafter *Heyns Report*].

14. *But see, e.g.*, Anthea Roberts & Sandesh Sivakumaran, *Lawmaking by Nonstate Actors: Engaging Armed Groups in the Creation of International Humanitarian Law*, 37 YALE J. INT'L L. 107, 109 (2012) ("[I]t is worth questioning whether nonstate armed groups can and should be given a role in the creation of the international law that governs conflicts to which they are parties.").

15. Statute of the International Court of Justice art. 38(1)(b), June 26, 1945, 59 Stat. 1031, 33 U.N.T.S. 993; *see generally* THE NATURE OF CUSTOMARY LAW: LEGAL, HISTORICAL AND PHILOSOPHICAL PERSPECTIVES (Amanda Perreau-Saussine & James Bernard Murphy eds., 2009).

16. MICHAEL P. SCHARF, CUSTOMARY INTERNATIONAL LAW IN TIMES OF FUNDAMENTAL CHANGE: RECOGNIZING GROTIAN MOMENTS 1 (2013). The attacks of 9/11 undoubtedly generated one such moment for *jus ad bellum*.

of IHL. In our view, States have underestimated this cost and must act to resume their intended role in the process.

I. *OPINIO JURIS*

State assessments of international law have long held a critical place in the law of nations. More than mere commentary, States' expressions of the perceived extent and content of their international legal obligations are key constitutive elements of international law. In particular, expressions of *opinio juris*, when combined with evidence of general State practice, form the basis of binding customary law.[17] Like treaties and general principles of law, customary law is a primary component of international law.[18] Absent meaningful and regular expressions of *opinio juris* by States, prospective customary law founders and extant customary law stagnates.

Opinio juris also animates the interpretation and application of IHL treaties.[19] As noted in Article 31(3) of the Vienna Convention on the Law of Treaties, "[a]ny subsequent practice in the application of the treaty which establishes the agreement of the parties regarding its interpretation" is a relevant consideration when interpreting a treaty's provisions.[20] *Opinio juris* serves as the vessel through which said agreement is revealed.[21] Moreover, when the context in which treaty provisions apply changes, subsequent expressions of *opinio juris* as to their application in the new environment, combined with corresponding State practice in their implementation, are the mechanisms by which treaty law remains relevant.[22]

Expressions of *opinio juris* are especially meaningful with respect to emerging domains of State interaction not anticipated when the present law emerged in the form of either treaty or customary law.[23] Few such domains rival cyber conflict in this regard.[24] It is understandable, therefore, that scholars and non-State organizations lavish attention on the question of how international law regulates cyber operations.[25] States, unfortunately, seem to be falling behind, continuing a trend that has been underway with respect to IHL generally for some time.[26]

---

17. Statute of the International Court of Justice art. 38(1)(b), June 26, 1945, 59 Stat. 1031, 33 U.N.T.S. 993; *see also* 1 OPPENHEIM'S INTERNATIONAL LAW 26 (Robert Jennings & Arthur Watts eds., 9th ed. 1996) [hereinafter OPPENHEIM] ("[T]he formulation in the [ICJ] Statute serves to emphasize that the substance of [international custom] of international law is to be found in the practice of states.").

18. *See* Statute of the International Court of Justice art. 38(1)(b), June 26, 1945, 59 Stat. 1031, 33 U.N.T.S. 993 (stating that the International Court of Justice should consult customary international law when resolving disputes).

19. *See* Yoram Dinstein, *The Interaction Between Customary International Law and Treaties*, 322 RECUEIL DES COURS 243 (2006) (discussing the relationship between treaties and customary international law).

20. Vienna Convention on the Law of Treaties art. 31(3)(b), May 23, 1969, 1155 U.N.T.S. 331.

21. *Id.*

22. *See generally id.*

23. *See id.* art. 38 ("Nothing in articles 34 to 37 precludes a rule set forth in a treaty from becoming binding upon a third State as a customary rule of international law, recognized as such.").

24. Michael N. Schmitt & Liis Vihul, *The Emergence of Legal Norms for Cyber Conflict*, *in* BINARY BULLETS: THE ETHICS OF CYBERWARFARE (Fritz Allhoff et al., 2015) (forthcoming).

25. *E.g.*, MARCO ROSCINI, CYBER OPERATIONS AND THE USE OF FORCE IN INTERNATIONAL LAW (2014); NATO COOP. CYBER DEF. CTR. OF EXCELLENCE, PEACETIME REGIME FOR ACTIVITIES IN CYBERSPACE: INTERNATIONAL LAW, INTERNATIONAL RELATIONS, AND DIPLOMACY (Katarina

II. *OPINIO JURIS* AVERSION

While there are frequently valid reasons for States' failure to offer clear, unequivocal indications of the practices they have undertaken or refrained from (or express their views on the actions of other States) out of a sense of international legal obligation,[27] risks attend inaction. Of greatest significance is the risk of legal vacuums left to be filled by actors who lack the de jure authority but not willingness to do so.

This willingness is especially evident with regard to IHL. Over recent decades, there has been a flurry of activity by non-State actors seeking to advance views of how IHL is to be interpreted and applied, and how it should develop.[28] Efforts by humanitarian and other non-governmental organizations, international tribunals, and academics have proved tremendously influential in this fecund normative environment,[29] one in which States have largely remained mute.[30] A brief examination of some of the more noteworthy instances illustrates the nature of this dynamic and presages how events may unfold if States do not engage proactively in the application of IHL to cyber operations during armed conflict.

The ICRC has led a number of recent efforts to clarify and progressively develop IHL.[31] More than a private humanitarian relief organization, the ICRC has long held a special place in the field.[32] It is commonly referred to as the "guardian of

---

Ziolkowski ed., 2013); Eric Talbot Jensen, *Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense*, 38 STAN. J. INT'L L. 207 (2002); Eric Talbot Jensen, *Unexpected Consequences from Knock-On Effects: A Different Standard for Computer Network Operations?*, 18 AM. U. INT'L L. REV. 1145 (2003); Michael N. Schmitt, *Rewired Warfare: Rethinking the Law of Cyber Attack*, 96 INT'L REV. RED CROSS (forthcoming) [hereinafter Schmitt, *Rewired Warfare*], *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2472800; Michael N. Schmitt, *The Law of Cyber Warfare:* Quo Vadis*?*, 25 STAN. L. & POL'Y REV. 269 (2014); Scott Shackelford, *From Nuclear War to Net War: Analogizing Cyber Attacks in International Law*, 27 BERKELEY J. INT'L L. 192 (2009).

26. *See, e.g.*, Roberts & Sivakumaran, *supra* note 14, at 108 (describing how States are "particularly hostile" to granting non-State actors any lawmaking power in international law); Schmitt, *Military Necessity*, *supra* note 10, at 811–14 (describing various States' apprehension regarding the adoption number of treaties adopted by international law).

27. *See, e.g.*, Sean Watts, *Reviving* Opinio Juris *and Law of Armed Conflict Pluralism*, JUST SECURITY (Oct. 10, 2013), http://justsecurity.org/1870/reviving-opinio-juris-law-armed-conflict-pluralism-2/ [hereinafter Watts, *Reviving* Opinio Juris] (explaining how an official of the federal government always prefaces his or her remarks with a "*pro forma* reminder that nothing [he or] she will say necessarily reflects the views" of his or her agency or the U.S. government on any international matters).

28. *See, e.g.*, Schmitt, *Military Necessity*, *supra* note 10, at 822 ("Nongovernmental organizations (NGOs) have increasingly moved from oversight and advocacy of human right into the field of international humanitarian law. In particular, a number of prominent organizations have begun to issue reports on IHL compliance during armed conflicts.").

29. *See, e.g.*, *id.* at 816–37 (describing how NGOs, international tribunals, and academic writings have influenced the development of international law).

30. *See, e.g.*, Watts, *Reviving* Opinio Juris, *supra* note 27 (describing how States' lack of participation in the dialogue regarding law of armed conflict is in contrast to the thriving commentary of non-States).

31. *See* Yves Sandoz, *The International Committee of the Red Cross as Guardian of International Humanitarian Law,* ICRC RESOURCE CTR. (Dec. 31, 1998) https://www.icrc.org/eng/resources/documents/misc/about-the-icrc-311298.htm ("In short, [the ICRC] has made a very direct contribution to the process of codification, during which its proposals were examined, and which has led to regular revision and extension of international humanitarian law . . . .").

32. *Id.*; *see generally* BOISSIER, *supra* note 6; ANDRÉ DURAND, HISTORY OF THE INTERNATIONAL

international humanitarian law."[33] Reflecting its mandate "to work for the understanding and dissemination of knowledge of international humanitarian law applicable in armed conflicts and to prepare any development thereof,"[34] the ICRC has recently published two highly influential studies and is in the process of producing a third.[35] Each has been, or is likely soon to be, viewed as a dependable expression of customary IHL, relied on by jurists and IHL practitioners, including State legal advisers.[36] Yet, as this Section will illustrate, the studies have provoked no serious response on the part of States and States have launched no comparable efforts of their own.

In 1995, the ICRC commissioned its Legal Division to conduct a large-scale study to codify "customary rules of IHL applicable in international and non-international armed conflicts."[37] Carried out over a span of ten years in consultation with over 150 legal experts, the resulting *Customary International Humanitarian Law* study (the Study) includes three volumes of work, running to well over 3,000 pages.[38] The Study is a work of breathtaking breadth and depth, one deeply rooted in a conscientious effort to discern State practice and *opinio juris* applicable to armed conflict.[39] It has been profoundly influential and is regularly cited by courts and commentators as authoritative on a number of points relating to the state of customary IHL.[40]

COMMITTEE OF THE RED CROSS: FROM SARAJEVO TO HIROSHIMA (1984); CAROLINE MOOREHEAD, DUNANT'S DREAM: WAR, SWITZERLAND AND THE HISTORY OF THE RED CROSS (1998).

33. Sandoz, *supra* note 31.

34. Statutes of the International Committee of the Red Cross art. 4(g), Oct. 3 2013, http://www.icrc.org /eng/resources/documents/misc/icrc-statutes-080503.htm.

35. 31st International Conference of the Red Cross and Red Crescent, Geneva, Nov. 28–Dec. 1, 2011, *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts*, 3, 31IC/11/5.1.2 (Oct. 2011) [hereinafter *ICRC Challenges*].

36. *See infra* note 41 and accompanying text; *cf.* Michael N. Schmitt, *The Law of Targeting*, *in* PERSPECTIVES ON THE ICRC STUDY ON CUSTOMARY INTERNATIONAL HUMANITARIAN LAW 131, 168 (Elizabeth Wilmshurst & Susan Breau eds., 2007) [hereinafter Schmitt, *Law of Targeting*] (discussing the acceptance by States of general targeting Rules set forth in the Study "as a correct enunciation" of targeting norms).

37. 26th International Conference of the Red Cross and Red Crescent, Geneva, Dec. 3–7, 1995, *International Humanitarian Law: From Law to Action-Report on the Follow-up to the International Conference on the Protection of War Victims*, Annex II, *in* 78 INT'L REV. RED CROSS 58, 84 (1996) [hereinafter ICRC, *From Law to Action*].

38. 1 INT'L COMM. OF THE RED CROSS, CUSTOMARY INTERNATIONAL HUMANITARIAN LAW (Jean-Marie Henckaerts & Louise Doswald-Beck eds., 2005) [hereinafter 1 CUSTOMARY IHL STUDY]; 2 INT'L COMM. OF THE RED CROSS, CUSTOMARY INTERNATIONAL HUMANITARIAN LAW (Jean-Marie Henckaerts & Louise Doswald-Beck eds., 2005) [hereinafter 2 CUSTOMARY IHL STUDY]; 3 INT'L COMM. OF THE RED CROSS, CUSTOMARY INTERNATIONAL HUMANITARIAN LAW (Jean-Marie Henckaerts & Louise Doswald-Beck eds., 2005) [hereinafter 3 CUSTOMARY IHL STUDY]; *see also* Jean-Marie Henckaerts, *Customary International Humanitarian Law: A Response to US Comments*, 89 INT'L REV. RED CROSS 473, 474 (2007) [hereinafter Henckaerts, *Response*]. Volume I of the Study features 161 Rules and accompanying commentary. 1 CUSTOMARY IHL STUDY. Volumes II and III compile an impressive catalogue of support for the Study's rules and commentary. 2 CUSTOMARY IHL STUDY; 3 CUSTOMARY IHL STUDY. An online database supplements these volumes, regularly updating its sourcing and citations. *Customary IHL: Practice*, ICRC, http://www.icrc.org/customary-ihl/eng/docs/v2 (last visited Apr. 30, 2015).

39. Yoram Dinstein, *The ICRC Customary International Humanitarian Law Study*, 36 ISR. Y.B. HUM. RTS. 1, 1 (2006).

40. *See e.g.*, *id.*

Considering the importance of the topics addressed, the comprehensiveness of its coverage, and the fact that the ICRC regularly informed States of its work, one might have expected the Study to rouse strong reactions from States, either in the form of approval or detailed disagreement therewith.[41] It did not. On the contrary, most States remained silent, thereby begging the question of whether the majority of States are of the view that the ICRC "got it right."

The United States was one of only a few States to respond to the Study. Shortly after publication, the Legal Adviser to the U.S. State Department and the General Counsel to the U.S. Department of Defense published a joint 22-page response to the ICRC President.[42] The letter, which purports only to review "a cross-section" of the Study, objects chiefly to the methodology used to identify customary international law, in particular alleging the Study affords too much weight to thin or selective samples of State practice.[43] The Legal Adviser and General Counsel also take issue with the Study's approach to *opinio juris*, noting that only "positive evidence . . . that States consider themselves legally obligated" can satisfy the *opinio juris* element of customary international law.[44]

Several of the letter's criticisms are compelling, especially with respect to the Study's reliance on non-binding instruments, such as United Nations General Assembly Resolutions and the ICRC's own prior work on IHL.[45] Overall, though, the letter lacks the thoroughness and heft expected of a response to such a significant and influential work. Indeed, only four pages of the letter provide general remarks,[46] with the remainder devoted to comments on just four rules: respect and protection of humanitarian relief personnel; protection of the environment; expanding bullets; and universal jurisdiction.[47] Many experts in the field were surprised the United States would issue such a letter and select only four relatively peripheral topics to address, while avoiding such core issues as the law governing attacks or detention.[48]

To be fair, the U.S. letter notes that the Study's length precluded a full review so soon after publication. The letter states, "The United States will continue its review and expects to provide additional comments or otherwise make its views known in due course."[49] Yet in the intervening eight years, the United States has

41. The Study provoked significant commentary from jurists and academic commentators. *See generally id.*; George H. Aldrich, *Customary International Humanitarian Law—An Interpretation on Behalf of the International Committee of the Red Cross*, 76 BRIT. Y.B. INT'L L. 503 (2005). Chatham House conducted a year long study on the Study that resulted in PERSPECTIVES ON THE ICRC STUDY ON CUSTOMARY INTERNATIONAL HUMANITARIAN LAW (Elizabeth Wilmshurst & Susan Breau eds., 2007).

42. John B. Bellinger III & William J. Haynes II, *A US Government Response to the International Committee of the Red Cross Study* Customary International Humanitarian Law, 89 INT'L REV. RED CROSS 443 (2007).

43. *Id.* at 444–45.

44. *Id.* at 447.

45. *E.g.*, *id.* at 457.

46. *See id.* at 443–46 (listing general marks about methodological concerns and international law principles).

47. *Id.* at 448–71

48. *See, e.g.*, Noura Erakat, *The U.S. v. the Red Cross: Customary International Humanitarian Law and Universal Jurisdiction*, 41 DENV. J. INT'L L. & POL'Y 225, 226 (2013) (comparing and contrasting the approach taken by the Red Cross and the approach favored in the U.S. response).

49. Bellinger & Haynes, *supra* note 42, at 444.

offered no further official comment on the Study and no such effort appears to be underway. Meanwhile, the Study continues to grow in influence, in great part because it remains the sole comprehensive work dedicated to discerning customary IHL available to jurists, scholars, and even State practitioners and legal advisors.[50] While the ICRC may lack the de jure competency to express *opinio juris*, in the absence of State action in that regard, the organization has de facto filled the void.

Between 2003 and 2008, the ICRC conducted a second major project aimed at developing and clarifying the legal consequences of civilian presence on the battlefield.[51] A succession of conflicts in the Balkans during the 1990s led to an infusion of civilians onto the battlefield, both participants from the region (e.g., armed groups of civilians) and civilian contractors associated with foreign armed forces.[52] Subsequent armed conflicts in Afghanistan and Iraq continued and even accelerated these trends.[53] In response, the ICRC decided in 2003 to examine the parameters of an important exception to the requirement that armed forces distinguish between civilians and combatants and only direct violence at the latter.[54] The exception provides that civilians lose their protection from attack for such time as they directly participate in hostilities.[55]

Participation in hostilities by civilians has long presented a host of humanitarian and tactical challenges.[56] Civilian fighters frequently fail to distinguish themselves visually from the surrounding civilian population,[57] a practice that frustrates the

---

50. *See generally* Schmitt, *Law of targeting*, *supra* note 36, at 134–35.

51. NILS MELZER, INT'L COMM. OF THE RED CROSS, INTERPRETIVE GUIDANCE ON THE NOTION OF DIRECT PARTICIPATION IN HOSTILITIES UNDER INTERNATIONAL HUMANITARIAN LAW 8 (2009) [hereinafter DPH GUIDANCE].

52. *See, e.g.*, Trevor A. Keck, *Not All Civilians Are Created Equal: The Principle of Distinction, the Question of Direct Participation in Hostilities and Evolving Restraints on the Use of Force in Warfare*, 211 MIL. L. REV. 115, 123–25 (2012) (discussing the increase in civilian casualties in the 1990s as well as the difficulties posed by humanitarian efforts during the Balkan wars).

53. *See, e.g.*, *id.* at 126–27 (citing Afghanistan for exemplifying the increase in civilian presence on the battlefield).

54. *Civilian "Direct Participation in Hostilities": Overview*, ICRC (Oct. 29, 2010), https://www.icrc.org/ eng/war-and-law/contemporary-challenges-for-ihl/participation-hostilities/overview-direct-participation.htm.

55. Protocol Additional to the Geneva Conventions of August 12, 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I) art. 51(3), June 8, 1977, 1125 U.N.T.S. 3 [hereinafter AP I]; Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II) art. 13(3), June 8, 1977, 1125 U.N.T.S. 609 [hereinafter AP II]. The notion of direct participation is widely viewed as customary in nature. For instance, the United States is a party to neither instrument, having ratified neither, but the concept appears in DEP'T OF THE NAVY ET AL., NWP 1-14M/MCWP 5-12.1/COMDTPUB P5800.7A, THE COMMANDER'S HANDBOOK ON THE LAW OF NAVAL OPERATIONS, 8-3 (2007) [hereinafter NWP 1-14M]. *See also* 1 CUSTOMARY IHL STUDY r. 6 (detailing civilians' loss of protection from attack). History can also be used to establish custom. *See* Keck, *supra* note 52, at 117 (stating that "the obligation to distinguish between combatants and non-combatants" has been recognized as early as the 5th century B.C.E.).

56. *See, e.g.*, HUM. RTS. WATCH, "BETWEEN A DRONE AND AL-QAEDA": THE CIVILIAN COST OF US TARGETED KILLINGS IN YEMEN 80–81 (2013) [hereinafter CIVILIAN COST] (discussing civilian casualties resulting from US targeted killings in Yemen).

57. This article uses the term "fighter" in lieu of "combatant" because combatancy is a concept involving issues of detention and belligerent immunity and has only derivative significance in the law of targeting. Moreover, the law of non-international armed conflict (NIAC) does not include a concept of

ability of armed forces to honor the foundational IHL principle of distinction.[58] Civilian fighters also regularly shift back and forth between peaceful activities and participation in hostilities—the so-called, "farmer-by-day-fighter-by-night" or "revolving door" dilemma—thereby raising the question of when such individuals may be attacked.[59] Although the challenge of how to deal with civilians on the battlefield was certainly not new in 2003,[60] the ICRC recognized the need to clarify the underlying law and accordingly convened a group of international law experts to consider the matter.[61] In 2008, the ICRC published the *Interpretive Guidance on the Notion of Direct Participation* (the *Guidance*) setting forth its views on the subject.[62]

The *Guidance*, and the process that produced it, examined the legal regime governing civilian direct participation in hostilities through the lens of the widely ratified 1977 Additional Protocols I and II (AP I for international armed conflict (IAC)[63] and AP II for non-international armed conflict (NIAC))[64] to the 1949 Geneva Conventions.[65] Articles in each of the Protocols provide: "Civilians shall enjoy the protection afforded by this section, unless and for such time as they take a direct part in hostilities."[66] Though undoubtedly an important concession to the realities of combat, and although all of the experts involved in the project agreed that the provisions accurately restated customary law,[67] these two brief articles have been exceptionally difficult to interpret and implement in practice.[68] The range of activities that constitute direct participation in hostilities and the temporal aspect of

---

combatancy. *Cf.* MICHAEL N. SCHMITT, CHARLES H.B. GARRAWAY & YORAM DINSTEIN, THE MANUAL ON THE LAW OF NON-INTERNATIONAL ARMED CONFLICT WITH COMMENTARY 4 (2006) [hereinafter NIAC MANUAL] (employing the term "fighters" as opposed to "combatants" to avoid confusion with international law of armed conflict)

58. AP I art. 48; DPH GUIDANCE, *supra* note 51, at 993.

59. DPH GUIDANCE, *supra* note 51, at 1034–36.

60. *See id.* at 993 (noting that there has been "[a] continuous shift of the conduct of hostilities into civilian population centres" in recent decades).

61. *Id.* at 991–92

62. *Id.* at 1034–37.

63. AP I art. 1(4).

64. AP II art. 1(1).

65. AP I; AP II. A number of militarily significant States have not ratified the Protocols including, *inter alia*, India, Indonesia, Iran, Israel, Malaysia, Pakistan, Singapore, Turkey, and the United States. On the U.S. position vis-à-vis particular provisions thereof, *see generally* George Cadwalader Jr., *The Rules Governing the Conduct of Hostilities in Additional Protocol I to the Geneva Conventions of 1949: A Review of the Relevant United States References*, *in* 14 Y.B. INT'L HUMAN. L. 133 (Michael N. Schmitt & Louise Arimatsu eds., 2011).

66. AP I art. 51(3); AP II art. 13(3).

67. In remarks in 1987, the Deputy Legal Adviser to the State Department, Michael J. Matheson, stated, "We . . . support the principle . . . that immunity [is] not be extended to civilians who are taking part in hostilities." Michael J. Matheson, Deputy Legal Advisor, U.S. Dep't of State, The United States Position on the Relation of Customary International Law to the 1977 Protocols Additional to the 1949 Geneva Convention, Remarks at the 6th Annual American Red Cross-Washington College of Law Conference on International Humanitarian Law (Jan. 2, 1987), *in* 2 AM. U. J. INT'L L. & POL'Y 419, 426 (1987).

68. *See id.* at 510 (noting Lieutenant Colonel Burrus M. Carnahan's statement that "[t]he main problem in interpreting these provisions is how much civilians must participate in the war effort before the Protocol no longer protects them" and that "[t]he standard of the Protocol . . . furnishes little clarification").

the exception were especially unclear to many Parties to the Protocols.[69] Of course, the same problems attend their interpretation and implementation in their customary guise for non-Parties to the Protocols such as the United States, Pakistan, India, and Israel.[70] Although the *Guidance* proposes understandings and interpretive glosses for both issues,[71] the ICRC was unable to secure unanimity thereon among the experts it had convened.[72] In fact, a group of notable experts withdrew from the project altogether in its final months.[73]

Expert dissent notwithstanding, the *Guidance*, as with the *Customary International Humanitarian Law* study before it, has been a markedly influential cynosure. For instance, it has found its way into military training for a number of NATO States and has affected the content of NATO rules of engagement in Afghanistan.[74] Despite these important practical effects, the *Guidance* has not attracted any definitive and comprehensive reaction from States. The scarcity of sovereign responses is especially curious and concerning with respect to States thought to disagree with aspects of the *Guidance*.

The United States has long embraced, albeit not publically by means of an expression of *opinio juris*, an understanding of direct participation and its consequences somewhat at odds with the *Guidance*. As an example, the *Guidance* asserts that there must be a direct causal link between the act in question and the harm caused to the enemy.[75] If an intervening event is required to effect harm, the civilian in question generally has not taken direct part in hostilities and retains protection from attack.[76] Most often cited in expert discussions as an example of how this approach would be implemented is the ICRC's characterization of assembly

69. *See* 1 CUSTOMARY IHL STUDY r. 6 ("It is fair to conclude . . . that outside the few uncontested examples . . . in particular use of weapons or other means to commit acts of violence against human or material enemy forces, a clear and uniform definition of direct participation in hostilities has not been developed in State practice.").

70. See for instance, discussion of the subject by the Israeli Supreme Court in HCJ 769/02 Pub. Comm. against Torture in Isr. v. Gov't of Isr. (2) IsrLR 459, 488–92 [2006], the holding of which is also summarized in Mark E. Wojcik, *Introductory Note to the Public Committee Against Torture in Israel v. The Government of Israel*, 46 I.L.M. 373 (2007).

71. DPH GUIDANCE, *supra* note 51, at 1012–37 (describing what constitutes direct participation in hostilities and the temporal scope of losing protection due to direct participation in hostilities).

72. *Id.* at 992.

73. For a published discussion on the points of contention by individuals who participated in the project, and an ICRC response thereto, see generally Bill Boothby, *"And for Such Time As": The Time Dimension to Direct Participation in Hostilities*, 42 N.Y.U. J. INT'L L. & POL. 741 (2010); Nils Melzer, *Keeping the Balance Between Military Necessity and Humanity: A Response to Four Critiques of the ICRC's Interpretive Guidance on the Notion of Direct Participation in Hostilities*, 42 N.Y.U. J. INT'L L. & POL. 831 (2010) [hereinafter Melzer, *Response*]; W. Hays Parks, *Part IX of the ICRC "Direct Participation in Hostilities" Study: No Mandate, No Expertise, and Legally Incorrect*, 42 N.Y.U. J. INT'L L. & POL. 769 (2010) [hereinafter Parks, *Part IX*]; Michael N. Schmitt, *Deconstructing Direct Participation in Hostilities: The Constitutive Elements*, 42 N.Y.U. J. INT'L L. & POL. 697 (2010) [hereinafter Schmitt, *Elements*]; Kenneth Watkin, *Opportunity Lost: Organized Armed Groups and the ICRC "Direct Participation in Hostilities" Interpretive Guidance*, 42 N.Y.U. J. INT'L L. & POL. 641 (2010).

74. *Cf.* Schmitt, *Elements*, *supra* note 73, at 699–732 (providing examples of how direct participation in hostilities influences military performance and conflicts in countries such as Iraq and Afghanistan).

75. DPH GUIDANCE, *supra* note 51, at 995–96.

76. *Id.* at 1022–23.

and storage of an improvised explosive device (IED) as *in*direct participation.[77] The contrary view is that the nexus between such activities and the subsequent IED attack renders those individuals engaging in the assembly and storage targetable as *direct* participants.[78] Although this position has not been expressed in the form of *opinio juris*, there is State practice in both Afghanistan and Iraq to suggest this is the U.S. position.[79]

Similar disagreement revolves around the issue of *when* civilians who participate in hostilities may be targeted. The *Guidance* states that the "for such time" language in the rules is limited to periods in which the civilian in question is actually engaging in "[m]easures preparatory to the execution of a specific act of direct participation in hostilities, as well as the deployment to and the return from the location of its execution."[80] It goes on to provide that "the 'revolving door' of civilian protection is an integral part, not a malfunction, of IHL."[81] In other words, the *Guidance* argues the "for such time" language should be interpreted literally as meaning that unless a civilian is then preparing the specific act, conducting it, or returning from that act, he or she is not targetable.[82] U.S. practice is not in accord.[83] From a military operational perspective, it seems irrational to prohibit targeting a civilian who has, perhaps on several occasions, conducted attacks on U.S. forces, and is likely to do so at some point in the future, merely because he or she has managed to return home following an operation and is not yet in the process of preparing a specific future attack.[84] Unfortunately, the United States has offered no clear expressions of *opinio juris* on the matter to accompany their practice.[85] In this void, the ICRC view is increasingly gaining traction.[86]

The issue of how to treat groups of civilian fighters, as distinct from individuals, also remains a point of contention. In the *Guidance*, the ICRC helpfully assimilates organized armed groups not meeting the requirements of combatant status to the armed forces for targeting purposes.[87] In other words, members of such groups may be targeted even when they are not directly participating in the hostilities.[88] And

---

77. *Id.* at 1021–22.

78. *See* Watkin, *supra* note 73, at 681 ("To limit direct participation to persons who place or detonate explosives is an artificial division of what is fundamentally a group activity.").

79. *Cf. id.* (explaining that the approach in the *Guidance* is impracticable in situations such as the insurgencies in Iraq and Afghanistan).

80. DPH GUIDANCE, *supra* note 51, at 1031.

81. *Id.* at 1035.

82. *See id.* at 1007–08 (indicating that the "determination remains subject to all feasible precautions and to the presumption of protection in case of doubt").

83. *Cf.* Matheson, *supra* note 67, at 420 (describing the U.S. policy to follow international guidance only when it is elevated to customary law status).

84. *See* Melzer, *Response*, *supra* note 73, at 879 ("[Air Commodore] Boothby contends that the [*Guidance*'s] interpretation of the temporal scope of direct participation in hostilities, and of the ensuing loss of protection, is too restrictive to make [] sense on the modern battlefield."(internal quotations omitted)).

85. *Cf.* Bellinger & Haynes, *supra* note 42, at 446–47 (describing US opposition to existence of *opinio juris* necessary to elevate principles in ICRC study to customary law).

86. *See* Melzer, *Response*, *supra* note 73, at 909–13 (identifying recent agreement of several States—including Israel—with some principles set forth in the DPH Guidance despite U.S. reservation).

87. DPH GUIDANCE, *supra* note 51, at 1006–09.

88. *Id.*

because they are targetable in the first place, any incidental harm to them caused during an attack on other persons or places would not qualify as collateral damage for the purposes of the proportionality and precautions in attack analyses.[89]

However, the *Guidance* restricts exposure to lawful targeting to those members having a "continuous combat function" in the group.[90] The parameters of the notion are roughly analogous to those of direct participation. By the *Guidance*'s approach, the "for such time" limitation does not apply to individuals who have a continuous combat function in an organized armed group; they may be attacked at any time irrespective of whether they are engaging in hostilities at the moment.[91] But for those members of the group who do not have such a function, the paradigmatic case being a cook who accompanies the fighters, the basic direct participation in hostilities rule for individuals applies such that they may only be attacked while so participating.[92]

The ICRC acceptance of the concept of a targetable organized armed group goes a long way towards meeting the long-standing U.S. concerns regarding the "revolving door."[93] Nevertheless, U.S. State practice neither limits targeting of a group's members to those with a continuous combat function nor requires harm to other members of the group to be considered in the proportionality or precautions in attack analysis when those with a continuous combat function are attacked.[94] On the contrary, such individuals would be treated analogously to members of the armed forces, that is, susceptible to lawful targeting based on mere membership in a group that has an express purpose of participating in the hostilities.[95] Given the importance of the issue vis-à-vis counterterrorist and counterinsurgency operations, one would have expected the United States to have staked out a firm position thereon. It has not, at least not in a manner that would constitute a clear expression of *opinio juris* on this important matter.[96]

States' interests in actively addressing the direct participation question are not limited to resolving interpretive challenges for purposes of targeting. The issue now appears to bear on other important IHL questions such as the use of civilian contractors to perform military functions more generally and whether civilian

89. *See* AP I arts. 51(5)(b), 57(2)(a)(iii), 57(2)(b) (describing generally precautions in attacks required under the protocol for civilians).

90. DPH GUIDANCE, *supra* note 51, at 1007–08

91. *See id.* at 1007 (observing that individual membership in an organized armed group is contingent on a continuous combat function).

92. *See id.* ("[U]nder IHL, the decisive criterion for individual membership in an organized armed group is whether a person assumes a continuous function for the group involving his or her direct participation in hostilities . . . .").

93. *See generally* W. Parks Hays, *Air War and the Law of War*, 32 A.F. L. REV. 1 (1990).

94. *See id.* at 118–31 (discussing the historical development of the concept of the "revolving door" and the United States' disagreement with it).

95. *Cf.* 1 CUSTOMARY IHL STUDY r. 6 (noting that the United States rejects a strict interpretation of the rule requiring the classification of an individual as a civilian when his status is in doubt and acknowledges a combatant's discretion in making such a classification).

96. *Cf.* Bellinger & Haynes, *supra* note 42, at 443–44 ("[T]he United States is not in a position to accept without further analysis that the [ICRC's] conclusions that particular rules related to the laws and customs of war in fact reflect customary international law.").

participation in hostilities constitutes an international war crime.[97] This trend, unsupported by the ICRC and most serious IHL experts, is counter-normative.[98] But more active State *opinio juris* on the direct participation question in general, and responses to the *Guidance* in particular, would greatly clarify matters.

A further incentive for States to respond actively to the *Guidance* can be found in a controversial provision on the resort to lethal force. The *Guidance* asserts that "the kind and degree of force which is permissible against persons not entitled to protection against direct attack must not exceed what is actually necessary to accomplish a legitimate military purpose in the prevailing circumstances."[99] Restated, attackers must resort to capture or other non-lethal means when feasible in the circumstances. As an example,

> an unarmed civilian sitting in a restaurant using a radio or mobile phone to transmit tactical targeting intelligence to an attacking air force would probably be regarded as directly participating in hostilities. Should the restaurant in question be situated within an area firmly controlled by the opposing party, however, it may be possible to neutralize the military threat posed by that civilian through capture or other non-lethal means without additional risk to the operating forces or the surrounding civilian population.[100]

The approach attracted significant pushback and criticism from numerous prominent IHL scholars.[101] Indeed, the "least harm" provision prompted several experts to withdraw from the project.[102] Moreover, the provision is at odds with many States' practice vis-à-vis conducting attacks and crafting rules of engagement.[103] While it is common for States to require their forces to capture when possible, such instructions are motivated by the operational need to acquire actionable intelligence, not by any sense that they are legally obligated to do so.[104] Yet, the *Guidance*'s discussion appears to have spawned a movement to entrench the

---

97. *See e.g.*, Mark David "Max" Maxwell & Sean Watts, *'Unlawful Enemy Combatant': Legal Status, Theory of Culpability, or Neither?*, 5 J. INT'L CRIM. JUST. 19, 20 (2007) (asserting that the classification of civilians as 'unlawful enemy combatants' confuses the distinct issues of legal status and culpability). *But see* David B. Rivkin, Jr. & Lee A. Casey, *The Use of Military Commissions in the War on Terror*, 24 B.U. INT'L L.J. 123, 131 (2006) (stating that the United States' stance that unlawful combatants are subject 'to trial and punishment by military tribunals' is not universally favored).

98. *See* 1 CUSTOMARY IHL STUDY r. 6 (stressing that a careful assessment of a civilian should be undertaken in determining his status and that attacks against civilians cannot be based on the civilian merely appearing dubious).

99. DPH GUIDANCE, *supra* note 51, at 1040.

100. *Id.* at 1043.

101. *See* Parks, *Part IX*, *supra* note 73, at 783–85 (detailing various experts' objections to the "General Restraints on the Use of Force in Direct Attack" section in the DPH Guidance).

102. *Id.* at 784–85.

103. *See id.* at 795–96 (noting that the ICRC requested the advice of senior military lawyers from the United States, United Kingdom, Israel, and Canada who disagreed with the provision on resort to lethal force and were ignored by the ICRC).

104. *See* Ryan Goodman, *The Power to Kill or Capture Enemy Combatants*, 24 EUR. J. INT'L L. 819, 824–25 (2013) (acknowledging that critics of the least harm provision contend that States commonly require their forces to capture, instead of kill, based on "pragmatic strategic and policy choices, not legal obligations").

least-harmful-means requirement in contemporary IHL understandings[105] and has sparked a lively academic debate.[106] Meanwhile, State input on the issue has been negligible.[107] It is worth considering whether States might have preempted the brouhaha with a more active and deliberate response to the *Guidance* in the form of an expression of *opinio juris*.

Finally with respect to ICRC efforts to develop IHL, a long-term project is underway within the ICRC Legal Division to produce updates to the 1949 Geneva Convention Commentaries (the Commentaries).[108] Originally published in the decade following the Conventions' entry into force,[109] the current edition of the Commentaries includes a volume addressing each of the four Conventions in significant detail, compiling essential historical perspective and details of diplomatic processes that produced the Conventions.[110] In 1987, the ICRC added a volume of similar commentary on the 1977 Protocols.[111] Altogether, the five volumes run to nearly 3,900 pages with commentary and doctrinal analysis of each of the articles of the four Conventions and their first two Additional Protocols.[112] The revised

105. *See, e.g.*, *id.* at 819 (arguing that "the use of force should instead be governed by a least-restrictive-means" analysis in certain well-specified and narrow circumstances).

106. *Compare* Geoffrey Corn et al., *Belligerent Targeting and the Invalidity of a Least Harmful Means Rule*, 89 INT'L L. STUD. 536, 540 (2013) (offering a comprehensive rebuttal of the least harmful means interpretation), *and* Michael N. Schmitt, *Wound, Capture, or Kill: A Reply to Ryan Goodman's 'The Power to Kill or Capture Enemy Combatants'*, 24 EUR. J. INT'L L. 855, 855 (2013) [hereinafter Schmitt, *Reply to Ryan Goodman*] (arguing that, even under narrow circumstances, there is no obligation under the extant international humanitarian law to wound rather than kill enemy combatants nor to capture rather than kill), *with* Ryan Goodman, *The Power to Kill or Capture Enemy Combatants: A Rejoinder to Michael N. Schmitt*, 24 EUR. J. INT'L L. 863, 863–66 (2013) (addressing the author's points of agreement and disagreement with Michael N. Schmitt's assertion that there exists no obligation under international humanitarian law to capture rather than kill enemy combatants), *and* Jens David Ohlin, *The Duty to Capture*, 97 MINN. L. REV. 1268, 1272 (2013) (examining four potential reasons why the duty to capture might be thought to apply to targeted killings).

107. *See* Schmitt, *Reply to Ryan Goodman*, *supra* note 106, at 857 ("[S]ituations presenting a viable possibility of wounding instead of killing are so rare that it is counter-intuitive to conclude that states intended the 'method' language to extend to such circumstances . . . [M]ost states, non-state organizations dealing with IHL, and scholars do not interpret the provision in this manner. For them, neither killing nor capture constitutes a specific method of warfare, although certain tactics designed to kill or capture do.").

108. Jean-Marie Henckaerts, *Bringing the Commentaries on the Geneva Conventions and Their Additional Protocols into the Twenty-First Century*, 94 INT'L REV. RED CROSS 1551, 1554 (2012) [hereinafter Henckaerts, *Twenty-First Century*].

109. *See id.* at 1552 ("[T]he International Committee of the Red Cross (ICRC) proceeded to write a detailed Commentary on each of their provisions. This led to the publication between 1952 and 1960 of a Commentary on each of the four Geneva Conventions . . . .").

110. *E.g.*, ICRC, COMMENTARY: GENEVA CONVENTION FOR THE AMELIORATION OF THE CONDITION OF WOUNDED, SICK AND SHIPWRECKED MEMBERS OF ARMED FORCES AT SEA (Jean S. Pictet ed., A.P. de Heney trans., 1960) [hereinafter COMMENTARY: GC II].

111. *See generally* ICRC, COMMENTARY ON THE ADDITIONAL PROTOCOLS OF 8 JUNE 1977 TO THE GENEVA CONVENTIONS OF 12 AUGUST 1949 (Yves Sandoz et al. eds., 1987) [hereinafter COMMENTARY ON THE ADDITIONAL PROTOCOLS].

112. *See generally* ICRC, COMMENTARY: GENEVA CONVENTION FOR THE AMELIORATION OF THE CONDITION OF THE WOUNDED AND SICK IN ARMED FORCES IN THE FIELD (Jean S. Pictet ed., 1952); ICRC, COMMENTARY: GENEVA CONVENTION RELATIVE TO THE PROTECTION OF CIVILIAN PERSONS IN TIME OF WAR (Jean S. Pictet ed., 1958); COMMENTARY: GC II, *supra* note 110; ICRC, COMMENTARY: GENEVA CONVENTION RELATIVE TO THE TREATMENT OF PRISONERS OF WAR (Jean S. Pictet ed., 1960) [hereinafter COMMENTARY: GC III]; COMMENTARY ON THE ADDITIONAL PROTOCOLS, *supra* note 111.

Commentaries will retain the format of their predecessors while significantly updating them with respect to interpretive developments and State practice.[113] They are expected to occupy a staff of full-time ICRC legal researchers and part-time external contributors through the year 2019.[114]

Also known as Pictet's Commentaries, after their lead editor Jean Pictet,[115] the Commentaries, together with the 1987 commentary on the Additional Protocols by Yves Sandoz et al., have been leading sources of clarification and background on the Conventions and Protocols for decades.[116] It is difficult to overstate their influential and nearly authoritative status. For instance, despite a clear disclaimer by the ICRC to the contrary, the United States Supreme Court recently cited the Commentaries as "the official commentaries" to the Geneva Conventions.[117] It is reasonable to expect that the forthcoming revised Commentaries will enjoy similarly influential and revered status as de facto "official" expositions on the ambiguities of the Conventions and their Protocols. At present, no State or collection of like-minded State legal advisors appears resolved or resourced to match this ICRC effort.[118]

Alongside the work of the ICRC, international criminal tribunals increasingly contribute to the development of IHL.[119] None has expounded on this body of law more actively or profusely than the International Criminal Tribunal for Former Yugoslavia (ICTY).[120] More than a criminal adjudicative body, the ICTY has

---

113. *See* Henckaerts, *Twenty-First Century*, *supra* note 108, at 1554 ("The update will preserve the format of the existing Commentaries . . . [and] will provide many references to practice, case law, and academic literature, which should facilitate further research and reading.").

114. *See id.* at 1554–55 (discussing the drafting process of the update to the Commentaries).

115. *See, e.g.*, W. Hays Parks, *Pictet's Commentaries*, *in* STUDIES AND ESSAYS ON INTERNATIONAL HUMANITARIAN LAW AND RED CROSS PRINCIPLES IN HONOR OF JEAN PICTET 495, 497 (Christophe Swinarski ed., 1984) (noting that "Pictet's 'Commentaries'—as they always are referred to—not only are of value because they are accessible; they are reliable").

116. *See* Henckaerts, *Twenty-First Century*, *supra* note 108, at 1553 (stating that "[o]ver the years, the ICRC Commentaries have come to be recognised as essential and well-respected interpretations of the Geneva Conventions and their Additional Protocols").

117. Hamdan v. Rumsfeld, 548 U.S. 557, 631 (2006). The Commentaries' editors were careful to observe that

> the Commentary is the personal work of its authors. The Committee moreover, whenever called upon for an opinion on a provision of an international Convention, always takes care to emphasize that only the participant States are qualified, through consultation between themselves, to give an official and, as it were, authentic interpretation of an intergovernmental treaty.

COMMENTARY: GC III, *supra* note 110.

118. *See generally* Henckaerts, *Twenty-First Century*, *supra* note 108.

119. *See* Jean-Marie Henckaerts, *Response*, *supra* note 38, at 486 (2007) (discussing the contribution to IHL from the courts in the former Yugoslavia, Rwanda, and Sierra Leone).

120. *See* Allison Marston Danner, *When Courts Make Law: How The International Criminal Tribunals Recast the Laws of War*, 59 VAND. L. REV. 1, 26 (2006) (stating that "the laws of war had developed faster since the beginning of the atrocities in the former Yugoslavia than in the forty-five years after the Nuremburg Tribunals" (citing Theodor Meron, Editorial Comment, *War Crimes Law Comes of Age*, 92 AM. J. INT'L L. 462, 463 (1998))); INT'L HUMAN. L. CLINIC, EMORY U. SCH. OF L., OPERATIONAL LAW EXPERTS ROUNDTABLE ON THE *GOTOVINA* JUDGMENT: MILITARY OPERATIONS, BATTLEFIELD REALITY AND THE JUDGMENT'S IMPACT ON EFFECTIVE IMPLEMENTATION AND ENFORCEMENT OF INTERNATIONAL HUMANITARIAN LAW 13 (2012) [hereinafter ROUNDTABLE], *available at* http://ssrn.com/abstract=1994414 (noting that "[i]ndeed, one of the mandates of the tribunal [ICTY] is the

enthusiastically embraced a law declaration function.[121] Since its earliest cases, the ICTY has offered exhaustive elaborations on perennially hazy IHL topics such as the threshold of armed conflict, the distinction between international and non-international armed conflict, and the range of persons protected by the Geneva Conventions.[122]

As an example, in *Prosecutor v. Gotovina,* an ICTY Trial Chamber issued a 1,377-page judgment that included highly controversial conclusions with respect to States' obligations when conducting attacks.[123] Based on those conclusions, the Chamber convicted two Croatian generals of war crimes related to artillery bombardments of urban areas.[124] Among other questionable findings, it concluded that shell craters located more than 200 meters from pre-planned military objectives in an urban area proved a criminal violation of the IHL principle of distinction.[125] The ICTY's Appeals Chamber reversed the convictions and rejected many of the Trial Chamber's characterizations of the principle.[126] The judgments set off a flurry of exchanges between respected IHL commentators concerning the relative merits of the Trial and Appeals Chambers' judgments.[127] States, however, were conspicuously absent from this important targeting and international criminal law dialogue.[128] Even States that frequently participate in armed conflict, and that would therefore be specially affected by the targeting standards at issue, declined to weigh in officially.[129]

---

progressive development of IHL").

121. *See* Danner, *supra* note 120, at 25–26 ("During the period of the [International Criminal Tribunal for the Former Yugoslavia's (ICTY)] greatest political weakness, its judges issued a surprising series of decisions that effected a fundamental transformation in the laws of war.").

122. *See, e.g.*, Prosecutor v. Tadić, Case No. IT-94-1-A, Appeals Chamber Judgment, para. 68–145 (Intl'l Crim. Trib. for the Former Yugoslavia July 15, 1999) (describing both when victims become protected persons under Art. 2, and when an internal armed conflict reaches the level of international armed conflict through the control of armed forces by a foreign power).

123. *See* ROUNDTABLE, *supra* note 120, at 4 ("Precisely because it is the only judgment addressing complex operational targeting considerations, the *Gotovina* case has the potential to be a great beacon for international law by adding significant definition to the legal paradigm that governs such targeting operations .... [H]owever, ... the legal analysis as presently conceived is flawed on multiple levels and therefore fails to achieve those goals."); *see generally* Prosecutor v. Gotovina, Case No. IT-06-90-T, Trial Chamber Judgment (Int'l Crim. Trib. for the Former Yugoslavia Apr. 15, 2011).

124. *Gotovina*, Case No. IT-06-90-T, para. 2588.

125. *Id.* para. 1899.

126. Prosecutor v. Gotovina, Case No. IT-06-90-A, Appeals Chamber Judgment, para. 83–87 (Int'l Crim. Trib. for the Former Yugoslavia Nov. 16, 2012).

127. *See, e.g.*, Prosecutor v. Gotovina, Case No. IT 06-90-A, Application and Proposed *Amicus Curiae* Brief concerning the 15 April 2011 Trial Chamber Judgment and Requesting that the Appeals Chamber Reconsider the Findings of Unlawful Artillery Attacks During Operation Storm, Conclusion (Int'l Crim. Trib. for the Former Yugoslavia Jan. 12, 2012) ("[A]ny judgment that is interpreted as attenuating this symmetry risks undermining the efficacy of international humanitarian law and the ultimate humanitarian objectives of the law."); Geoffrey S. Corn & Lt. Col. Gary P. Corn, *The Law of Operational Targeting: Viewing the LOAC Through an Operational Lens*, 47 TEX. INT'L L.J. 337, 339 (2012) (discussing the effect of Gotovina on the "interrelationship between law and military doctrine"); ROUNDTABLE, *supra* note 120, at 2 (criticizing the "potential flaws in the Trial Chamber's application of IHL; and ... potential institutional concerns and second-order effects resulting from these flaws").

128. *See generally* Corn & Corn, *supra* note 127; ROUNDTABLE, *supra* note 120.

129. *E.g.*, Jamila Trindle, *Acquitted in Court, Still Blacklisted by the U.S.*, FOREIGN POLICY (Jan. 10, 2014), http://www.foreignpolicy.com/articles/2014/01/10/acquitted-in-court-still-blacklisted-by-the-u-s.

This was not always the case. The ICTY's early IHL work provoked meaningful State involvement.[130] For example, in 1995 the U.S. Department of State filed an amicus curiae brief in the Tribunal's first case, *Tadić*.[131] The brief outlined U.S. legal views on the threshold of armed conflict, characterization of armed conflicts as either IAC or NIAC, availability of the grave breaches enforcement regime in NIAC, and nature and content of the laws and customs of war.[132] The brief continues to serve as a reliable expression of *opinio juris*.[133] Yet, since its filing, the United States has not participated meaningfully and substantively in other war crimes cases, nor has it offered a similarly thorough or reasoned reaction to a judgment of any international criminal tribunal.[134] The reasons for this inactivity are unclear, but the growing list of States party to the International Criminal Court and that Court's expanding caseload suggest that militarily active States would be well-advised to engage in the development of IHL through war crimes tribunals, lest they find themselves governed on the battlefield by legal norms developed in isolation by jurists.

The IHL advocacy efforts of NGOs are of similarly worthy note. For instance, Human Rights Watch (HRW), one of the most sophisticated of NGOs dealing with IHL, regularly issues reports on ongoing or recent conflicts.[135] The organization also takes strong advocacy positions on IHL-related matters.[136] An example is its 2013 *Losing Humanity* report, which argued, *inter alia*, that autonomous weapon systems are unlawful per se under IHL.[137] Although individual scholars protested at such an overbroad (and incorrect) statement,[138] no State has addressed the various IHL

130. *See* Danner, *supra* note 120, at 21–22 (noting that the Representative of Venezuela issued a report expressing the view that the Tribunal would not be empowered with setting the norms of International Law while Canada argued for more specifics in what fell under ICTY jurisdiction).

131. Submission of the Government of the United States of America Concerning Certain Arguments Made by Counsel for the Accused in the Case of The Prosecutor of the Tribunal v. Dusan Tadić (July 27, 1995) [hereinafter U.S. *Tadić* Amicus], *available at* http://www.state.gov/documents/organization/65825.pdf.

132. *See id.* at 27–37 (arguing that the Tribunal had jurisdiction over grave breaches, violations of customs of war, and crimes against humanity because the alleged offenses did occur during an international armed conflict).

133. *See* Watts, *Reviving* Opinio Juris, *supra* note 27 (observing the brief's contribution to a "more pluralistic, balanced, and active LOAC dialogue").

134. *Id.*

135. *E.g.*, HUM. RTS. WATCH, TURNING A BLIND EYE: IMPUNITY FOR LAWS-OF-WAR VIOLATIONS DURING THE GAZA WAR (2010), *available at* http://www.hrw.org/node/89575.

136. *See, e.g.*, HUM. RTS. WATCH, LOSING HUMANITY: THE CASE AGAINST KILLER ROBOTS 1–2 (2012) [hereinafter LOSING HUMANITY], *available at* http://www.hrw.org/sites/default/files/reports/arms1112 ForUpload_0_0.pdf (advocating for a ban on fully autonomous weapons); HUM. RTS. WATCH, TIME FOR JUSTICE: ENDING IMPUNITY FOR KILLINGS AND DISAPPEARANCES IN 1990S TURKEY 61–63 (2012), *available at* http://www.hrw.org/sites/default/files/reports/turkey 0912ForUpload.pdf (recommending further steps the Turkish government needs to take to combat impunity in Turkey).

137. LOSING HUMANITY, *supra* note 136, at 1.

138. *See, e.g.*, Kenneth Anderson et al., *Adapting the Law of Armed Conflict to Autonomous Weapon Systems*, 90 INT'L L. STUD. 386, 387 (2014) (suggesting prohibiting autonomous weapons would be "misguided"); Marco Sassóli, *Autonomous Weapons and International Humanitarian Law: Advantages, Open Technical Questions and Legal Issues to Be Clarified*, 90 INT'L L. STUD. 308, 309–10 (2014) (contending that an autonomous weapon can reasonable comply with IHL); Michael N. Schmitt, *Autonomous Weapon Systems: A Reply to the Critics*, HARV. NAT'L SECURITY J. FEATURES (Feb. 2013)

matters the organization raised head on.[139] Instead, the United States issued a Department of Defense Directive that places certain policy limitations on the systems without offering meaningful comment on the relevant legal issues.[140] Such failure to engage the topic cedes control of the legal discourse to organizations such as HRW and the chapeau organization in the campaign against autonomous systems, Stop Killer Robots.[141]

United Nations bodies have also entered the fray in various instances, including appointments by the Human Rights Council of Special Rapporteurs on countering terrorism (Mr. Ben Emmerson) and extrajudicial, summary, or arbitrary executions (Mr. Christof Heyns).[142] Both have issued reports on drone operations, including IHL issues, marked by a high degree of sophistication and normative detail.[143] Although the United States is actively involved in drone operations, it has issued no comprehensive statement on the legal questions surrounding drone strikes. Instead, the government's limited comments tend to be made, as will be discussed, in speeches by senior government officials at academic and professional gatherings or found in internal memoranda not intended to be made public.[144]

Finally, scholars and other IHL experts have convened and collaborated with increasing frequency to produce legal manuals devoted to restating customary and treaty IHL, and in many cases clarifying difficulties concerning its application and operation.[145] Topics covered by these manuals include the law of naval warfare, non-

---

at 1–3 (arguing *Losing Humanity* "obfuscates the on-going legal debate over autonomous weapon systems").

139. *See* Matthew Waxman & Kenneth Anderson, *Don't Ban Armed Robots in the U.S.*, NEW REPUBLIC, Oct. 17, 2013, http://www.newrepublic.com/article/115229/armed-robots-banning-autonomous-weapon-systems-isnt-answer (arguing that States should engage in cooperative development of common standards and best practices within a law of war framework).

140. *See* U.S. DEP'T OF DEF., DIRECTIVE NO. 3000.09, AUTONOMY IN WEAPONS SYSTEMS (2012), *available at* http://www.dtic.mil/whs/directives/corres/pdf/300009p.pdf (setting broad limitations and guidelines regarding the use of autonomous weapons systems).

141. CAMPAIGN TO STOP KILLER ROBOTS, http://www.stopkillerrobots.org/ (last visited Apr. 18, 2015).

142. *See Drone Attacks: UN Experts Express Concern About the Potential Illegal Use of Armed Drones*, U.N. HUMAN RIGHTS: OFFICE OF THE HIGH COMM'R FOR HUMAN RIGHTS (Oct. 25, 2013), http://www.ohchr.org/en/ NewsEvents/Pages/DisplayNews.aspx?NewsID=13905 (explaining involvement of Emmerson and Heyns as U.N. Special Rapporteurs and noting their roles). The most recent mandates for the Special Rapporteurs are, respectively, Human Rights Council Res. 22/8, Protection of Human Rights and Fundamental Freedoms While Countering Terrorism: Mandate of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, 22nd Sess., Mar. 21, 2013, A/HRC/RES/22/8 (Apr. 9, 2013), and Human Rights Council Res. 26/12, Mandate of the Special Rapporteur on Trafficking in Persons, Especially Women and Children, 26th Sess., June 20, 2014, A/HRC/26/L.23 (June 20, 2014).

143. *Emmerson Report*, *supra* note 13, at 5; *Heyns Report*, *supra* note 13, at 8.

144. *E.g.*, Harold Honhgu Koh, Legal Adviser, U.S. Dep't of State, The Obama Administration and International Law, Remarks at the Annual Meeting of the American Society of International Law (Mar. 25, 2010) [hereinafter Koh, American Society Remarks], *available at* http://www.state.gov/s/l/releases/remarks/139119.htm.

145. *E.g.*, SAN REMO MANUAL ON INTERNATIONAL LAW APPLICABLE TO ARMED CONFLICTS AT SEA (Louise Doswald-Beck ed., 1995) [hereinafter SAN REMO MANUAL]; PROGRAM ON HUMANITARIAN POLICY AND CONFLICT RESEARCH AT HARVARD UNIV., HPCR MANUAL ON INTERNATIONAL LAW APPLICABLE TO AIR AND MISSILE WARFARE (2009) [hereinafter HPCR MANUAL]; NIAC MANUAL; *see also* PROGRAM ON HUMANITARIAN POLICY AND CONFLICT RESEARCH AT HARVARD UNIV.,

international armed conflict law, and the law of air and missile warfare.[146] Each is widely cited in legal literature and has influenced practice in its respective field.[147] And each appears to have responded to concerns that participating experts harbored regarding the failure of States to provide legal practitioners sufficiently granular guidance on troublesome IHL issues.[148] Although these manuals were not intended to supplant the role of States in IHL interpretation and development, they are, to a degree, having exactly that effect.

In sum, it is clear that States have not kept pace with an ever-increasing flow of non-State international legal commentary; the volume and frequency of the latter drowns out what little comment and reaction States have offered. It is no exaggeration to say that jurists, NGOs, scholars and other non-State actors presently have greater influence on the interpretation and development of IHL than do States. The roles of the respective communities have, unfortunately, been reversed—the pluralistic process of formation and development that has long guaranteed the efficacy and relevance of IHL is in peril.

III. THE ROLE OF STATES

Notwithstanding their recent reserve with respect to *opinio juris*, States and their legal agents still enjoy unique relevance in the formation and interpretation of international law generally and IHL in particular. As the primary authors and subjects of IHL, States have authority to actively shape its content and direction, through both direct means, such as treaty formation and State practice, and indirect means, such as positions proffered in litigation, legal publications, public statements of legal intent, and diplomatic communications resorting to law.[149]

Even as scholars challenge State-centric understandings of international law, near universal respect endures for the special role of sovereigns in the formation of international law.[150] To co-opt and modify a common observation with respect to Originalism in American constitutional interpretation, everyone is a sovereigntist sometimes.[151] What distinguishes dyed-in-the-wool international law sovereigntists

---

COMMENTARY ON THE HPCR MANUAL ON INTERNATIONAL LAW APPLICABLE TO AIR AND MISSILE WARFARE (2010) [hereinafter HPCR MANUAL WITH COMMENTARY].

146. *See generally* HPCR MANUAL; NIAC MANUAL; SAN REMO MANUAL.

147. *See, e.g.*, Wolff Heintschel von Heinegg, *The Current State of the Law of Naval Warfare: A Fresh Look at the* San Remo Manual, 82 INT'L L. STUD. 269, 269 (2006) (analyzing the influence of the *San Remo Manual* on current policies and addressing the manual's shortcomings); *see also Symposium: The 2009 Air and Missile Warfare Manual: A Critical Analysis*, 47 TEX. INT'L L. J. 261, 261–379 (2012) (discussing in detail the Manual on International Law Applicable to Air and Missile Warfare).

148. HPCR MANUAL foreword; NIAC MANUAL preface; SAN REMO MANUAL introductory note.

149. *See* 1 OPPENHEIM, *supra* note 17, at 26 ("[Custom may be] evidenced by such internal matters as [States'] domestic legislation, judicial decisions, diplomatic despatches, internal government memoranda, and ministerial statements in Parliaments and elsewhere.").

150. *See, e.g.*, Christoph Schreuer, *The Waning of the Sovereign State: Towards a New Paradigm for International Law?*, 4 EUR. J. INT'L L. 447, 448 (1993) (mentioning the importance of State structure in the future development of international law while prognosticating the end of a traditional model of sovereignty for States).

151. David A. Strauss, *The Living Constitution*, REC. ONLINE (ALUMNI MAG.) (Fall 2010), http://www.law.uchicago.edu/alumni/magazine/fall10/strauss ("[A]s a matter of rhetoric, everyone is an originalist sometimes . . . .").

from non-sovereigntists is probably not acceptance of the legitimacy of State input, but rather attitudes toward non-State actors' international legal contributions. Few international lawyers contest that State expressions of *opinio juris* constitute legitimate sources of law and a principled form of international legal interpretation.[152] Disagreements seem instead to concern the effect that absence of State *opinio juris* has on an international norm.[153] And while there is surely value in the balanced pluralism that results from having both State and non-State contributions to the interpretation and development of international law, State input has always been singularly significant, particularly when armed conflict is the issue.[154] State *opinio juris* remains the critical bellwether for the degree of consensus, acceptance, and therefore effectiveness and legitimacy of any international legal rule.

In addition to formal authority, States possess unique competency, facility, and access with respect to the contextual ingredients of international law.[155] IHL is illustrative. Many commentators grasp the harsh consequences of armed conflict.[156] Yet, few outside the ambit of States' defense ministries and armed forces fully appreciate the operational challenges, demands, and limitations of combat so essential to fairly striking the delicate balance between military necessity and humanity that infuses IHL and informs its interpretation and evolution.[157] Even commentators with a military or military legal background can find that their IHL experiential base has become dated or passé.[158] There is truly no adequate substitute for the active input of IHL professionals immersed in States' current operations and legal deliberation.

The dearth of contextual IHL custom and States' viewpoints is often unavoidable. States frequently shield their battlefield conduct and decision making from public view for rational operational reasons.[159] And although they may acquire information concerning the practices of adversaries and other States by employing intelligence, surveillance, and reconnaissance (ISR) assets, that information is

152. *See* Eric Engle, *U.N. Packing the State's Reputation? A Response to Professor Brewster's "Unpacking the State's Reputation"*, 114 PENN ST. L. REV. PENN STATIM 34, 37 (2010) (operating under the assumption that international law is enforced by states).

153. *See* Ross E. Schreiber, *Ascertaining* Opinio Juris *of States Concerning Norms Involving the Prevention of International Terrorism: A Focus on U.N. Process*, 16 B.U. INT'L L.J. 309, 312 (1998) (detailing the difficult task of deducing *opinio juris*).

154. *See id.* (detailing the particular confusions that arise when trying to deduce international norms without State *opinio juris*, particularly in armed, nuclear conflict).

155. *See* Ingrid Wuerth, *The Alien Tort Statute and Federal Common Law: A New Approach*, 85 NOTRE DAME L. REV. 101, 110 (2010) (bolstering an argument by stating that international law relies on a State's domestic laws and that a State actor's courts applying the State's own law is "normatively superior").

156. *See, e.g.*, Ariel Zemach, *Taking War Seriously: Applying the Law of War to Hostilities Within an Occupied Territory*, 38 GEO. WASH. INT'L L. REV. 645, 646–47 (describing the human costs of war in Iraq and the Gaza Strip).

157. *See id.* at 675–76 (assessing the intricacies present in balancing human rights with the demands of wartime).

158. *See* Olivier Bangerter, *Reasons Why Armed Groups Choose to Respect International Humanitarian Law or Not*, 93 INT'L REV. RED CROSS 353, 370 (2011) ("[I]t is questionable how far knowledge of the content of IHL by many commanders and fighters really extends beyond some basic notions.").

159. *See, e.g.*, Laura K. Donohue, *The Shadow of State Secrets*, 159 U. PA. L. REV. 77, 88–91 (2010) (discussing frequency and challenges of State military secrets).

typically classified and therefore unavailable to non-State actors. States do regularly share some classified information amongst themselves, the paradigmatic examples being "five-eyes" sharing[160] and the sharing of classified material among NATO allies,[161] but, because release would reveal certain "sources and methods" of collection, non-State actors seldom see such material, for better or worse, except when it is leaked.[162] The practical effect of this restricted informational environment is to stymy non-State efforts to discern State practices, thereby rendering the former's input to the IHL interpretation and development process, through no fault of their own, somewhat suspect.

Additionally, the reluctance of States to express *opinio juris* on particular topics of international law is in some senses understandable. A number of considerations recommend the increasingly prevalent wait-and-see approach. A State may conclude that too little is known about the implications of an emerging area of warfare to commit to any particular international regulatory doctrine or regime or to admit publicly to the existence of international norms bearing on the matter at all. It is also possible that State reticence is less the product of calculated caution rather than political impasse deriving from domestic political considerations. In many municipal legal systems, constitutional and statutory arrangements spread authority over international law matters among several agencies and even branches of government, frustrating coordination and consensus.[163] Interagency friction or disagreement may prevent government-level consensus, especially with respect to new or emerging legal debates.

Absence of expressed State *opinio juris* may even be explained as evidence of *opinio juris* itself.[164] In such a case, the State may intend its silence as an implied expression of the view that no relevant IHL norm exists.[165] Restated, although a State may undertake a continuous course of practice on the battlefield, that same State may assiduously refrain from accompanying expressions of *opinio juris* so as to preclude any purported crystallization of a customary norm. This might be the case, for example, when it imposes self-defense limits on the use of force in rules of

160. *See* Paul Farrell, *History of 5-Eyes–Explainer*, THE GUARDIAN (Dec. 2, 2013), http://www.theguardian.com/world/2013/dec/02/history-of-5-eyes-explainer (delineating the history of the five-eyes partnership, involving intelligence sharing between the U.S., U.K., Canada, Australia, and New Zealand).

161. *See generally* Alasdair Roberts, *Entangling Allies: NATO's Security of Information Policy and the Entrenchment of State Secrets*, 36 CORNELL INT'L L.J. 329 (2003).

162. *See* Afsheen John Radsan & Richard Murphy, *Measure Twice, Shoot Once: Higher Care for CIA-Targeted Killing*, 2011 U. ILL. L. REV. 1201, 1216–18, 1236 (2011) (detailing the relationship between the government's interest in preventing disclosure of sources and methods and the public's interest especially in the judicial context).

163. For example, the U.S. Constitution vests authority over international law to each of the branches of the federal government. *See* U.S. CONST. art. I, § 8, cl. 10 (enumerating the U.S. Congress's power to "define and punish offenses against the law of Nations"); *id.* art. II, § 2, cl. 2 (requiring Senate advice and consent for treaty ratification); *id.* (enumerating the U.S. President's power "to make Treaties"); *id.* art. III, § 2, cl. 1 (extending the judicial power to "all Cases, in Law and Equity, arising under . . . Treaties").

164. *But see* MARTTI KOSKENNIEMI, FROM APOLOGY TO UTOPIA: THE STRUCTURE OF INTERNATIONAL LEGAL ARGUMENT 437 (2006) ("It is impossible to make any presumptions about the *opinio juris* on the basis of such silence as a matter of *general rule*.").

165. *Contra id.*

engagement in situations in which status-based targeting is lawful or when it affords treatment to detainees in excess of what IHL would otherwise require.

On balance, however, the various rationales for State restraint on matters of *opinio juris* are overrated. State silence has not proved effective at stemming IHL's development, which appears to occur with or without active State involvement.[166] Plainly, the failure of States to produce or interpret specific rules of conduct for emerging areas of warfare has not counseled silence on the part of non-State legal actors.[167] They have aggressively stepped in to cultivate IHL in response to the vacuum left by States.[168] Rather than preserve operational and legal flexibility, State silence may simply cede significant initiative and power over IHL to non-State actors.

Two international legal controversies demonstrate how State delay, ambiguity, or silence with respect to *opinio juris* risks the imposition of very real costs. Soon after the al Qaeda terrorist attacks of September 11, 2001, the United States launched military operations in Afghanistan "in order to prevent any future acts of international terrorism against the United States."[169] U.S. armed forces soon captured individuals believed to be affiliated with al Qaeda or organizations that were said to have supported or harbored al Qaeda, such as Afghanistan's de facto Taliban government.[170] By early 2002, U.S. armed forces and intelligence agencies had transferred over 150 suspected high-level leaders or valuable fighters to the U.S. military base at Guantanamo Bay, Cuba.[171]

Questions concerning the legal status of the Guantanamo detainees quickly arose.[172] Some speculated the detainees might qualify as prisoners of war, entitled to the protections of the Third Geneva Convention of 1949.[173] Others contended that both al-Qaeda and Taliban members were extra-legal persons and unlawful combatants, entitled to no specific international legal protections.[174] The U.S. government did little to quell or resolve debate.[175] Its public position on the matter

166. *See* 1 CUSTOMARY IHL STUDY xlv–xlvi (stating that a state omission or abstention *may* be construed to support *opinion juris*).

167. *See supra* Part II.

168. *Id.*

169. Authorization for Use of Military Force (AUMF), Pub. L. No. 107-40, 115 Stat. 224 (2001) (codified at 50 U.S.C. § 1541 (2006)).

170. *See* 1 CTR. FOR LAW & MILITARY OPERATIONS, U.S. ARMY, LEGAL LESSONS LEARNED FROM AFGHANISTAN AND IRAQ, VOLUME I: MAJOR COMBAT OPERATIONS (11 SEPTEMBER 2001–1 MAY 2003), at 53 (2004) (describing legal issues concerning enemy personnel detained in Afghanistan in late 2001).

171. *See* Katharine Q. Seelye, *Troops Arrive at Base in Cuba to Build Jails*, N.Y. TIMES, Jan. 7, 2002, http://www.nytimes.com/2002/01/07/us/a-nation-challenged-the-prisoners-troops-arrive-at-base-in-cuba-to-build-jails.html (detailing the number of prisoners present in Cuba in 2002 as over 300).

172. Bryan Bender, *Red Cross Disputes US Stance on Detainees*, BOSTON GLOBE, Feb. 9, 2002, at A1 [hereinafter *U.S. Stance*]; *Agency Differs with U.S. over P.O.W.'s*, N.Y. TIMES, Feb. 9, 2002, http://www.nytimes.com/2002/02/09/international/09DETA.html.

173. Bender, *supra* note 172, at A1.

174. *E.g.*, Sean D. Murphy, *Decision Not to Regard Persons Detained in Afghanistan as POWs*, 96 AM. J. INT'L L. 475, 476–77 (2002).

175. *See* Kim Lane Scheppele, *Law in A Time of Emergency: States of Exception and the Temptations of 9/11*, 6 U. PA. J. CONST. L. 1001, 1030–34 (2004) (describing the ways in which the Bush Administration approached handling the legal status of terrorists captured and detained post-9/11).

was vague, especially as to the underlying legal reasoning upon which its actions were purportedly based.[176]

This is not to say the government had ignored the issue of the detainees' international legal status. As public and political debate swirled, a parallel, albeit cloistered, legal debate took place within and between several U.S. executive branch agencies.[177] The various positions broadly emulated those that had surfaced in public debate within the broader legal community.[178] However, at the time, the government neither publically proffered a comprehensively-reasoned legal analysis of its detention policy, nor provided any clear statement setting forth its views on U.S. legal obligations regarding the Guantanamo detainees' status and treatment.[179]

In early 2002, President Bush ultimately settled the internal executive branch debate on the detainees' legal status.[180] However, the full legal bases for the government's ultimate position remained classified.[181] The Bush administration appeared satisfied to justify its determinations of the detainees' legal status with short summary fact sheets.[182] In fact, the full legal reasoning analyzing the detainees' status was never made public through any officially approved expression of *opinio juris*—it was instead leaked.[183] As the unauthorized release of photos depicting prisoner abuse at the Abu Ghraib military detention facility in Iraq took place in April 2004,[184] news outlets also began to receive and publish leaked copies of executive branch legal documents and memoranda addressing the Guantanamo detainees' legal status and the justifications for their indefinite detention.[185] The leaked memoranda fueled intense debate, litigation, and resentment, both in the

176. *Id.*

177. *See generally* THE TORTURE PAPERS: THE ROAD TO ABU GHRAIB (Karen J. Greenberg & Joshua L. Dratel eds., 2005) [hereinafter THE TORTURE PAPERS]. The Papers are a compilation of dozens of U.S. government legal memoranda and investigations related to detainee policies in the Global War on Terrorism. *See generally id.*

178. *Id.*

179. *See* Murphy, *supra* note 174, at 477 (describing the Bush administration's changing stance on the status and treatment of Guantanamo detainees under the Geneva Convention).

180. Memorandum from President George W. Bush for Vice President, et al., Humane Treatment of Taliban and Al Qaeda Detainees (Feb. 7, 2002) [hereinafter Memo. from President Bush], *available at* http://www.pegc.us/archive/White_House/bush_memo_20020207_ed.pdf; *see also* Katharine Q. Seelye, *In Shift, Bush Says Geneva Rules Fit Taliban Captives*, N.Y. TIMES, Feb. 8, 2002, http://www.nytimes.com/2002/02/08/world/nation-challenged-captives-shift-bush-says-geneva-rules-fit-taliban-captives.html (reporting that the decision to apply of the Geneva Convention to Taliban captives ended an "internal legal debate").

181. *A Guide to the Memos on Torture*, N.Y. TIMES, http://www.nytimes.com/ref/international/24MEMO-GUIDE.html?_r=0 (last visited Apr. 28, 2015).

182. Fact Sheet, White House Press Office, Status of Detainees at Guantanamo (Feb. 7, 2002), *available at* http://www.presidency.ucsb.edu/ws/?pid=79402; *see also*, Press Release, Dep't of Def., DoD News Briefing: Secretary Rumsfeld and Gen. Myers (Feb. 12, 2002), *available at* http://www.defense.gov/transcripts/transcript.aspx?transcriptid=2636 (demonstrating Secretary Rumsfeld's failure to expand on the Administration's reasoning when questioned).

183. Memo. from President Bush, *supra* note 180.

184. *See* Seymour M. Hersh, *Torture at Abu Ghraib*, THE NEW YORKER, May 10, 2004, *available at* http://www.newyorker.com/magazine/2004/05/10/torture-at-abu-ghraib (breaking the story of prisoner abuse by military personnel).

185. *See generally* THE TORTURE PAPERS, *supra* note 177.

United States and abroad.[186] They also inspired international lawyers to aggressively rebut the legal reasoning contained therein.[187] The U.S. executive branch quickly lost the initiative regarding characterization of the detainees' status under IHL to the judicial branch, Congress, and even the non-State international law community.

To be sure, not all of the negative fallout of the affair is attributable to absence of effective *opinio juris*. Substantive deficiencies in the legal analyses of the memoranda supporting the policies are chiefly to blame.[188] The marginalization of seasoned professional legal expertise within the executive branch likewise contributed.[189] Yet, a more vigorous and public approach to *opinio juris* could have prevented much of the costly fallout. If U.S. executive branch officials felt it necessary to abandon long-settled principles with respect to the classification and treatment of persons detained in armed conflict, an active and public campaign of timely and tightly-reasoned *opinio juris* would surely have been a more effective way to develop international norms better suited to the modern security needs of States than secretive, unilaterally constructed memoranda. If the laws-of-war were indeed "quaint" and "obsolete" in some respects,[190] a carefully managed campaign of *opinio juris* that marshaled the full expertise and resources of the U.S. government's legal community would surely have proved more successful in updating them in both the long and short term.

The expanding use of drones to target terrorists outside active theaters of combat operations is a second instance where the United States appears to prefer to operate under a shroud of legal ambiguity.[191] These operations raise questions from an array of legal regimes—the *jus ad bellum*, sovereignty, human rights, and IHL.[192] With respect to IHL, the core issues are 1) whether the drone operations are being mounted as an aspect of an "armed conflict" such that IHL applies and, if so, 2) whether the individuals attacked qualify as lawful targets, and 3) whether the

186. *See, e.g.*, Arthur H. Garrison, *The Bush Administration and The Office of Legal Counsel (OLC) Torture Memos: A Content Analysis of the Response in the Academic Legal Community*, 11 CARDOZO PUB. L. POL'Y & ETHICS J. 1, 11–12, 6–26 (2012) (discussing the academic community's moral indignation).

187. *Id.* at 6.

188. *Id.* at 6–7.

189. *See, e.g.*, Lt. Col. Paul E. Kantwill & Maj. Sean Watts, *Hostile Protected Persons or "Extra-Conventional Persons": How Unlawful Combatants in the War on Terrorism Posed Extraordinary Challenges for Military Attorneys and Commanders*, 28 FORDHAM INT'L L.J. 681, 682–83 (2005) (discussing the role of judge advocates in giving legal advice to the ranking commander in Iraq at the time of the Abu Ghraib detainee abuses).

190. Draft Memorandum from Alberto Gonzales, White House Counsel, to George W. Bush, Decision re Application of the Geneva Convention on Prisoners of War to the Conflict with al Qaeda and the Taliban (Jan. 25, 2002), *reprinted in* THE TORTURE PAPERS, *supra* note 177, at 118.

191. CIVILIAN COST, *supra* note 56, at 80–81.

192. *Id.* at 26, 80–83; Rotem Giladi, *The* Jus Ad Bellum/Jus in Bello *Distinction and the Law of Occupation*, 41 ISR. L. REV. 246, 246–47 (2008) ("Every . . . practitioner of international humanitarian law (IHL) is familiar with the distinction between *jus ad bellum* and *jus in bello* (or IHL). Both are public international law regimes that regulate war but whereas the former regulates the *legality* of the use of force *per se*, the latter concerns the legality of the *manner* in which force is used. The distinction generally means that the rules of *jus in bello* apply irrespective of questions of legality under *jus ad bellum* and that, as a consequence, all belligerents are subject to the same rules of *jus in bello*, whatever their position under *jus ad bellum*.").

operations comply with IHL rule of proportionality and the requirement to take precautions in attack.[193]

There is no question that the admixture of normative regimes renders linear and compartmentalized legal analysis of the drone program challenging.[194] Indeed, much of the discussion to date has misstated the law and conflated separate and distinct legal regimes.[195] It is a discourse that has been marked by emotive assertions as much as by legal acumen.[196] However, non-State actors have lately started to produce analyses that are sophisticated and convincing.[197] Noteworthy in this regard are recent reports by HRW, Amnesty International, and the two U.N. Special Rapporteurs, all of which, appropriately so, have garnered significant attention in the international law community.[198]

Yet to date, the government, under two very different administrations, has offered no thorough expression of *opinio juris* that draws together the various legal strands in a manner that would convincingly justify the strikes as a matter of international law.[199] Instead, both administrations have resorted to periodic speeches by senior officials who provide only vague glimpses of the U.S. position.[200]

Most often cited is a speech by former Department of State Legal Adviser Harold Koh at the 2010 Annual Meeting of the American Society of International Law.[201] Although heralded at the time as the first full explanation of U.S. legal policy on drone strikes, for experts in the field it was a rather confusing explication.[202] For instance, it was unclear whether the use of force against members of al Qaeda was being justified on the basis of the law of self-defense (a *jus ad bellum* issue), because of U.S. involvement in an armed conflict with the organization (an IHL issue), or on account of both.[203] The speech was likewise unexceptional. An

---

193. AP I arts. 51(5)(b), 57(2)(a)(iii), 57(2)(b); 1 CUSTOMARY IHL STUDY r. 14–24.

194. *See generally* Michael Schmitt, *Narrowing the International Law Divide: The Drone Debate Matures*, 39 YALE J. INT'L L. ONLINE 1, 3 (2014) [hereinafter Schmitt, *Drone Debate*].

195. *Id.* at 3–9.

196. *Id.*

197. *See id.* at 12–13 (describing analysis and comparison of prominent recent reports)

198. *See generally Emmerson Report*, *supra* note 13; *Heyns Report*, *supra* note 13; CIVILIAN COST, *supra* note 56; AMNESTY INT'L, "WILL I BE NEXT?": US DRONE STRIKES IN PAKISTAN (2013) [hereinafter DRONE STRIKES IN PAKISTAN]. For an analysis of the four reports, see generally Schmitt, *Drone Debate*, *supra* note 194.

199. *See, e.g.*, DRONE STRIKES IN PAKISTAN, *supra* note 198, at 49 (describing the refusal of the United States to provide public access to information about its drone program in Pakistan).

200. *See, e.g.*, John B. Bellinger III, Legal Adviser, U.S. Dep't of State, Address at the London School of Economics: Legal Issues in the War on Terrorism (Oct. 31, 2006) [hereinafter Bellinger, War on Terrorism], *available at* http://www.state.gov/s/l/2006/98861.htm (describing the U.S. views on the detention and treatment of terrorists since 9/11).

201. Koh, American Society Remarks, *supra* note 144.

202. *See, e.g.*, COLUMBIA LAW SCH. HUM. RTS. INST., TARGETING OPERATIONS WITH DRONE TECHNOLOGY: HUMANITARIAN LAW IMPLICATIONS 2 (2011) (discussing former Department of State Legal Adviser Harold Koh's explanation of U.S. legal policy on drone strikes and the legality of U.S. practice).

203. Koh, American Society Remarks, *supra* note 144, at 7. Adviser Harold Koh stated, "[a]s I have explained, as a matter of international law, the United States is in an armed conflict with al-Qaeda, as well as the Taliban and associated forces, in response to the horrific 9/11 attacks, and may use force consistent with its inherent right to self-defense under international law." *Id.*

announcement that the United States complies with the principle of distinction and the rule of proportionality hardly constitutes an epiphany.[204] Failure to comply would not only violate IHL, but also amount to a war crime by those involved.[205] And curiously, there is no mention of the requirement to take precautions in attack, which is central to the legality of drone strikes under IHL.[206]

Other noteworthy speeches include those by Koh's predecessor, John Bellinger, at the London School of Economics;[207] John Brennan at Harvard Law School while he was serving as the President's Assistant for Counterterrorism;[208] Attorney General Eric Holder at Northwestern University School of Law;[209] former Defense Department General Counsel Jeh Johnson at Yale Law School;[210] and the President himself at National Defense University.[211] A brief Fact Sheet was released by the White House contemporaneously with the President's speech.[212] Each of these addressed particular aspects of IHL and other bodies of law governing drone operations, but none offered an analysis robust enough to draw any but the broadest of conclusions as to the U.S. view of the applicable law.[213] Moreover, the speeches not only failed to clearly distinguish the various legal regimes from which the relevant law derives, but left it uncertain whether the positions taken were the product of legal, operational, moral, or policy concerns. Paradoxically, the most comprehensive analysis by the government of the international law issues surrounding drone operations was that offered in an unsigned and undated draft Justice Department White Paper that was leaked to the press in 2013, hardly an exemplar of reliable *opinio juris*.[214]

---

204. Koh, American Society Remarks, *supra* note 144, at 7–8.

205. *See* 1 CUSTOMARY IHL STUDY r. 1, 14, 156 (discussing the principle of distinction between civilians and combatants, proportionality in attack, and definition of war crimes, respectively).

206. *See generally* Koh, American Society Remarks, *supra* note 144 (lacking discussion of drone precautionary measures); *see also ICRC Challenges*, *supra* note 35, at 38–39 (discussing required precautions under IHL and its application to drone attacks).

207. Bellinger, War on Terrorism, *supra* note 200.

208. John O. Brennan, Asst. to the President for Homeland Sec. & Counterterrorism, Strengthening Our Security by Adhering to Our Values and Laws, Remarks at the Program on Law and Security at Harvard Law School (Sept. 16, 2011), *available at* http://www.whitehouse.gov/the-press-office/2011/09/16/remarks-john-o-brennan-strengthening-our-security-adhering-our-values-an.

209. Eric Holder, U.S. Att'y Gen., Remarks at Northwestern University School of Law (Mar. 5, 2012), *available at* http://www.justice.gov/iso/opa/ag/speeches/2012/ag-speech-1203051.html.

210. Jeh Charles Johnson, Gen. Counsel, U.S. Dep't of Def., National Security Law, Lawyers and Lawyering in the Obama Administration, Address at the Dean's Lecture at Yale Law School (Feb. 22, 2012), *in* 31 YALE L. & POL'Y REV. 141 (2012).

211. President Barack Obama, Remarks by the President at the National Defense University (May 23, 2013), http://www.whitehouse.gov/the-press-office/2013/05/23/remarks-president-national-defense-university.

212. Fact Sheet: The President's May 23 Speech on Counterterrorism, White House Press Office (May 23, 2013), https://www.whitehouse.gov/the-press-office/2013/05/23/fact-sheet-president-s-may-23-speech-counterterrorism.

213. *See generally id.*; Bellinger, War on Terrorism, *supra* note 200; Brennan, *supra* note 208; Holder, *supra* note 209; Johnson, *supra* note 210; Obama, *supra* note 211.

214. *See generally* U.S. Dep't of Justice, Lawfulness of a Lethal Operation Directed Against a U.S. Citizen Who is a Senior Operational Leader of Al-Qa'ida or an Associated Force (Leaked Draft White Paper Nov. 8, 2011), *available at* http://msnbcmedia.msn.com/i/msnbc/sections/news/020413_DOJ_White_Paper.pdf.

The vacuity of recent *opinio juris* is particularly surprising given the fact that the law of drone operations is exceedingly emotive and has underpinned widespread and impassioned condemnation of the United States as a "might makes right" State.[215] As a matter of law, the basis for the U.S. operations is arguably sound.[216] Articulating that basis publicly would not only have the immediate effect of tempering the criticism (much of which is levied on the basis of a lack of legal transparency[217]), but also help preserve the option of conducting drone operations extraterritorially in the future.

Whatever the reason for the U.S. failure to issue an unambiguous expression of *opinio juris*, by now the United States and other countries that conduct such operations have lost control of the debate. Non-State actors are shaping the discussion as they wish, with States merely responding, or more often not responding at all, to the sundry objections they raise.[218] From this reactive stance, it is nearly impossible for States conducting drone strikes to muster sufficient support from other States to redirect the debate. The domestic political costs of supporting the strikes (at least those outside an active battlefield) are simply too high for them.[219] Additionally, the United States has not provided an adequately detailed and reasoned delineation of its legal position that could be assessed and embraced by other States.[220] To employ military terminology, the drone debate and many other currently debated IHL issues are, for the United States especially, "self-inflicted wounds."

Perhaps the most pressing need for an expression of *opinio juris* is with respect to those articles of AP I the United States believes accurately reflect customary law—and those it does not. The instrument was designed to supplement the four 1949 Geneva Conventions, which dealt primarily with protections for specified persons and objects.[221] Rules regarding how combat was to occur were the province of the 1907 Regulations annexed to Hague Convention IV.[222] Although a post-

---

215. *See generally* CIVILIAN COST, *supra* note 56 (detailing the civilian casualties of U.S. drone policy and recommending changes).

216. *See generally* Michael N. Schmitt, *Extraterritorial Lethal Targeting: Deconstructing the Logic of International Law*, 52 COLUM. J. TRANSNAT'L L. 77 (2013).

217. *See, e.g.*, Letter from the American Civil Liberties Union et al. to President Barack Obama (Dec. 4, 2013) [hereinafter Letter to President Obama], *available at* http://justsecurity.org/wp-content/uploads/2013/12/2013-12-04-Coalition-Follow-Up-Letter-to-Obama-on-TK.pdf (calling on the government to "publicly disclose key targeted killing standards and criteria"); MICAH ZENKO, COUNCIL ON FOREIGN RELATIONS, COUNCIL SPECIAL REPORT NO. 65: REFORMING U.S. DRONE STRIKE POLICIES 3 (2013) (stating that the "lack of transparency threatens to limit U.S. freedom of action and risks proliferation of armed drone technology without the requisite normative framework"); *Heyns Report*, *supra* note 13, at 21 (emphasizing to the U.N. the need for greater transparency regarding drone policy for all states).

218. *See, e.g.*, Koh, American Society Remarks, *supra* note 144, at 7–8 (responding to criticisms against U.S. targeting practices); Letter to President Obama, *supra* note 217 (noting President Obama's stated intention to limit the use of lethal force).

219. *See* ANTHONY DWORKIN, EUROPEAN COUNCIL ON FOREIGN RELATIONS, DRONES AND TARGETED KILLING: DEFINING A EUROPEAN POSITION 2–4 (2013) (discussing domestic opposition to drone strikes among E.U. member States).

220. *See* Letter to President Obama, *supra* note 217 (asking for a clearer standard for drone strikes); ZENKO, *supra* note 217, at 16–17 (noting that the United States has offered multiple legal justifications for drone strikes).

221. AP I art. 1(3).

222. Hague Convention (IV) Respecting the Laws and Customs of War on Land, Oct. 18, 1907, 36

World War II tribunal at Nuremberg found that it reflected customary law,[223] the treaty was sparse and clearly in need of expansion in the aftermath of two world wars and numerous post-World War II conflicts such as those in Algeria and Vietnam.[224] AP I, addressed to international armed conflict, was intended to serve that process.[225] In the ensuing two and a half decades, the United States has remained a non-Party.[226] Still, 174 States are Party to the Protocol, including most NATO allies and States with which the United States frequently operates militarily, such as Canada, the United Kingdom, and Australia.[227]

To date, the United States has issued no comprehensive expression of *opinio juris* regarding those provisions of AP I it regards as reflecting customary international law.[228] Although it is clear from U.S. practice, training, and doctrine that certain key provisions, such as the proportionality aspects of Articles 51 and 57, are accepted as customary,[229] little is known beyond that. For instance, does the United States accept the definition of perfidy only with the exclusion of the reference to "capture," as is sometimes asserted?[230] Does it continue to take the position that the provisions on the environment do not reflect customary law? Is the U.S. position on military objectives that "war-sustaining" objects are included, as appears to be the case from the Navy/Marine Corps/Coast Guard manual, but which has been criticized as a distortion of the law?[231] What is the current U.S. position regarding combatant status for those members of a militia group belonging to a Party to the conflict, but who do not wear distinguishing attire or symbols when conducting an attack?[232]

When trying to discern the U.S. legal position with respect to these and other unsettled issues, scholars and practitioners turn to three sources. The first two are internal Department of Defense memoranda, one to the Chairman of the Joint Chiefs of Staff,[233] the other to an Assistant General Counsel.[234] Both cover the same

---

Stat. 2277, 1 Bevans 631.

223. United States v. von Leeb et al. [High Command Trial], 11 TRIALS OF WAR CRIMINALS BEFORE THE NUERNBERG MILITARY TRIBUNALS UNDER CONTROL COUNCIL LAW NO. 10, at 532 (1950).

224. *See* George Aldrich, *New Life for the Laws of War*, 75 AM. J. INT'L L. 764, 764 (1981) (noting that the Additional Protocols were created to address the deficiencies in the Geneva Conventions).

225. *Id.*

226. *Treaties and States Party to Such Treaties*: *Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977*, ICRC, https://www.icrc.org/applic/ihl/ihl.nsf/States.xsp?xp_viewStates=XPages_NORMStatesParties&xp_treatySelected=470 (last visited Apr. 8, 2015) [hereinafter *ICRC Additional Protocol Parties*].

227. *Id.*

228. *See generally* Theodor Meron et al., Customary Law and Additional Protocol I to the Geneva Conventions for Protection of War Victims: Future Directions in Light of the U.S. Decision Not to Ratify, Panel Discussion, *in* 81 AM. SOC'Y INT'L L. PROC. 26 (1987).

229. *Cf.* Koh, American Society Remarks, *supra* note 144 (discussing the rigorous implementation of proportionality and distinction throughout the planning and execution of lethal operations in the Obama Administration).

230. *See* AP I art. 37 (stating the prohibition of perfidy elements).

231. NWP 1-14M, *supra* note 55, para. 8.2; YORAM DINSTEIN, THE CONDUCT OF HOSTILITIES UNDER THE LAW OF INTERNATIONAL ARMED CONFLICT 95–96 (2d ed. 2010).

232. *See* AP I art. 44 (reciting the rule under the Protocol Additional to the Geneva Conventions).

233. Memorandum to the Chairman of the Joint Chiefs of Staff on Protocols I and II–Humanitarian Law during Armed Conflict, Office of the Ass't Sec'y of Def., (Nov. 7, 1977) [hereinafter Memorandum to the Chairman] (on file with author).

ground and are distinguished by their brevity and restatement of the obvious.[235] The third is a speech by the then Deputy Legal Adviser of the State Department at an academic conference in 1987 that was reprinted in the *American University Journal of International Law and Policy*.[236] To provide guidance to its judge advocates, the U.S. Army has reprinted the second memorandum and a summary of the article in its current 2014 *Law of Armed Conflict Documentary Supplement*.[237]

This lack of *opinio juris* is problematic. U.S. forces have been at war over a decade with little official guidance as to those aspects of AP I, the most comprehensive conduct of hostilities treaty, the United States believes are customary in nature.[238] Moreover, in both of its major conflicts, U.S. troops operated alongside forces subject to the Protocol and in many cases commanded those troops in combat, thereby raising important questions of legal interoperability.[239]

Finally, especially illustrative of the U.S. reluctance to set forth its IHL positions openly is the tortured process to produce a Department of Defense (DoD) Law of War Manual.[240] Although military manuals are not themselves expressions of *opinio juris* because they are often based in part on operational and policy concerns, they serve as useful evidence thereof.[241] Presently, the Army Manual dates from

234. Memorandum from W. Hays Parks et al. to Mr. John H. McNeill, Ass't Gen. Counsel, Office of the Sec'y of Def. (May 9, 1986), *in* U.S. ARMY JUDGE ADVOCATE GEN.'S LEGAL CTR. & SCH., LAW OF ARMED CONFLICT DOCUMENTARY SUPPLEMENT 234–35 (William J. Johnson ed., 2014) [hereinafter Memorandum to John H. McNeil].

235. *Compare* Memorandum to the Chairman, *supra* note 233, *with* Memorandum to John H. McNeil, *supra* note 234, at 234-35 (listing the provisions of the 1977 Protocols Additional to the Geneva Conventions that were already part of customary international law).

236. Matheson, *supra* note 67; *see also* Abraham D. Sofaer, Legal Adviser, U.S. Dep't of State, Remarks on the Position of the United States on Current Law of War Agreements (Jan. 22, 1987), *in* 2 AM. U. J. INT'L L. & POL'Y 460, 467–68 (1987) (discussing why the Joint Chiefs of Staff found AP I to be "militarily unacceptable").

237. U.S. ARMY JUDGE ADVOCATE GEN.'S LEGAL CTR. & SCH., LAW OF ARMED CONFLICT DOCUMENTARY SUPPLEMENT 232–35 (William J. Johnson ed., 2014).

238. *See* Cadwalader, *supra* note 65, at 135 ("Unfortunately, there is no single authoritative reference detailing those provisions of AP I the US accepts as an accurate restatement of customary international law or other legal obligations, or that it follows as a matter of policy during armed conflict.").

239. The U.S. has not ratified AP I, but many States that have assisted the U.S. in armed conflicts over the past decade have ratified AP I. *ICRC Additional Protocol Parties*, *supra* note 226.

240. *See* W. Hays Parks, Update on the DOD Law of War Manual, Address before the American Bar Association Standing Committee on National Security, at 6 (Nov. 30 2012) [hereinafter Parks, Update on the DOD Law of War Manual], *available at* http://www.lawfareblog.com/wp-content/uploads/2012/12/Parks.Manual.pdf (detailing the failure of the 2010 draft of the manual); Robert Chesney, *Hays Parks on the Demise of the DOD War Manual*, LAWFARE (Dec. 8 2012), http://www.lawfareblog.com/2012/12/hays-parks-on-the-demise-of-the-dod-law-of-war-manual/ ("The effort to publish that manual now appears to be dead in the water, for better or worse, and the speech Hays gave at last week's meeting is something of a post-mortem providing his view as to why things stalled."); Edwin Williamson & Hays Parks, *Where is the Law of War Manual?*, 18 WKLY. STANDARD (July 22, 2013), http://www.weeklystandard.com/articles/where-law-war-manual_739267.html?nopager=1 (discussing both the fourteen year process of drafting the manual as well as the sudden thirty month delay in approving the manual); Cadwalader, *supra* note 65, at 156 (stating that "the author of this paper has been informed that the Manual remains under review and its release date is uncertain").

241. *See* Cadwalader, *supra* note 65, at 160–68 (interpreting AP I in light of the Army Field Manual and the Navy/Marine Corps/Coast Guard Manual).

1956,[242] the Navy/Marine Corps/Coast Guard Manual is a 2007 product,[243] and the Air Force no longer has a manual in force.[244] In 1996, the Army Judge Advocate General's sensible proposal that a manual be produced for all four DoD services was accepted.[245] It took nearly a decade and a half to produce a draft,[246] a particularly unfortunate pace given that two major wars replete with extraordinarily complex legal issues were underway for much of the period. Acceptance of the draft appears to have become the victim of interagency disagreement.[247]

As a result, the Army operates armed with a manual that is 58 years old and the Air Force "flies and fights" without any comprehensive published legal guidance.[248] In the absence of formal guidance, U.S. forces are sometimes forced to train, operate, and render legal advice based on documents issued by non-State actors, including some of those mentioned *supra*.[249] The situation is regrettable not only for its failure to support serving military lawyers and commanders, but also as yet another example of U.S. retreat from active IHL *opinio juris*.

IV. CYBER *OPINIO JURIS*

Clearly, the absence of authoritative State *opinio juris* impoverishes IHL discussions, debates, and deliberations, both descriptive and normative. Whatever one's opinion of the substantive quality or correctness of a State's particular expression of *opinio juris*, State legal opinions provide indispensable control samples for meaningful analysis and critique. The efforts of, inter alia, legal practitioners, judges, government legal advisers, scholars, commanders, humanitarian workers, members of the media, and policy makers inexorably suffer when States fail to clarify and update their views on the content, interpretation, and future direction of IHL.

The question is, of course, whether the unfortunate tendency of States to shy away from expressions of *opinio juris* will continue to plague IHL? It is a question of seminal importance in light of new forms and means of warfare. Of these, the emergence of cyberspace as a pervasive aspect of conflict[250] presents the most

242. DEP'T OF THE ARMY, FIELD MANUAL 27-10: THE LAW OF LAND WARFARE (1956) [hereinafter FM 27-10].

243. *See generally* NWP 1-14M, *supra* note 55.

244. The Air Force manual has been rescinded. DEP'T OF THE AIR FORCE, JUDGE ADVOCATE GEN., AIR FORCE PAMPHLET 110-34, COMMANDER'S HANDBOOK ON THE LAW OF ARMED CONFLICT (1980).

245. Williamson & Parks, *supra* note 240.

246. *See id.* (remarking that the Department of Defense (DoD) working group spent fourteen years to produce the first draft of the manual).

247. *See id.* (explaining major policy disagreements among Departments of State, Justice, and Defense); *see also* Parks, Update on the DOD Law of War Manual, *supra* note 240 (indicating consensus of the agencies involved after the first draft of the manual was produced in 2010 has since ended). *But see* Letter from Robert S. Taylor, Acting General Counsel, Dep't of Def. to Editor of The Weekly Standard (July 18, 2013), *available at* http://www.lawfareblog.com/wp-content/uploads/2013/07/Letter-to-The-Weekly-Standard_18Jul2013.pdf (responding to the Williamson and Parks article *supra* note 240 and emphasizing that experts are still working cooperatively and diligently to produce the final version of the manual).

248. *See* FM 27-10, *supra* note 242 (dating from July 1956); *see* DEP'T OF THE AIR FORCE, *supra* note 244 (noting the Army Manual was written in 1956 and the Air Force manual has been rescinded).

249. *E.g.*, *Emmerson Report*, *supra* note 13.

250. *See, e.g.*, DEP'T OF DEFENSE, STRATEGY FOR OPERATING IN CYBERSPACE 2–4 (J2011)

pressing demand for *opinio juris*. Indeed, States' armed forces have been quick to embrace cyberspace as a domain of military operations.[251]

Cyber operations began to capture the attention of the international legal community in the 1990s.[252] However, the terrorist attacks of September 11, 2001, refocused attention on the law of counterterrorism and the law governing the counterinsurgency operations that came to characterize the conflicts in Afghanistan and Iraq.[253] It was not until the massive cyber operations directed against Estonia in 2007, following that State's movement of a Soviet-era statue commemorating the "Great Patriotic War,"[254] and the use of such operations during the international armed conflict between Russia and Georgia the following year,[255] that the legal community began examining the topic of cyber law again.[256]

Initially, there was disagreement whether IHL applied at all to cyber operations given their non-kinetic nature.[257] Assertions of non-applicability, however, fly in the face of the object and purpose of IHL. For instance, Article 36 of AP I mandates a review of new methods and means of warfare prior to their use.[258] The requirement to review new means (weapons) is generally deemed to reflect customary law.[259] And, as recently acknowledged by the "Group of Governmental Experts" representing fifteen countries convened by the U.N. General Assembly, international

---

[hereinafter STRATEGY FOR OPERATING IN CYBERSPACE], *available at* http://www.defense.gov/news/d20110714cyber.pdf (describing various threats and potential vulnerabilities posed by malicious cyber attacks that could affect military, public, and private interests); JOINT CHIEFS OF STAFF, JOINT PUBLICATION 3-13, INFORMATION OPERATIONS vii (2012), *available at* http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf [hereinafter INFORMATION OPERATIONS] ("The nation's state and non-state adversaries are equally aware of the significance of this new technology, and will use information-related capabilities . . . to gain advantages in the information environment, just as they would use more traditional military technologies to gain advantages in other operational environments.").

251. *See, e.g.*, STRATEGY FOR OPERATING IN CYBERSPACE, *supra* note 250, at 5 ("Though the networks and systems that make up cyberspace are man-made, often privately owned, and primarily civilian in use, treating cyberspace as a domain is a critical organizing concept for DoD's national security missions. This allows DoD to organize, train, and equip for cyberspace as we do in air, land, maritime, and space to support national security interests."); *see generally* INFORMATION OPERATIONS, *supra* note 250.

252. The first conference on the subject was held at the U.S. Naval War College in 1999. *See generally Computer Network Attack and International Law*, 76 INT'L L. STUD. intro. (2002).

253. *See, e.g.*, Bellinger, War on Terrorism, *supra* note 200 (discussing changes in counterterrorism law and policy in the War on Terrorism since September 11, 2001).

254. *See, e.g.*, ENEKEN TIKK ET AL., COOP. CYBER DEF. CTR. OF EXCELLENCE, INTERNATIONAL CYBER INCIDENTS: LEGAL CONSIDERATIONS 15, 18–20 (2010), *available at* http://www.ccdcoe.org/publications/books/legalconsiderations.pdf (providing a history and overview of the 2007 cyber attacks on Estonia).

255. *Id.* at 67–79.

256. *Id.* at 79.

257. *See, e.g.*, *id.* at 79–86 (discussing the applicability of international law to the Georgia conflict).

258. AP I art. 36.

259. *See* TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE r. 48 (Michael N. Schmitt ed., 2013) [hereinafter TALLINN MANUAL] (identifying a review requirement as customary international law). Although some States do not acknowledge the customary nature of the norm vis-à-vis methods of warfare, this minor deviation from the text of Article 36 has little bearing on the general applicability of IHL to cyber operations.

law applies to cyber activities.[260] There is quite simply no cogent reason to exclude IHL from the ambit of applicable international law.[261]

Although a majority of States, including the United States, appears to regard the existing IHL as the primary source of duties and obligations during cyber conflict,[262] no comprehensive treaty regime as of yet specifically regulates such situations.[263] There appears to be no political stomach on the part of States for adopting such treaties in the foreseeable future. As a result, the main focus of legal activity will inevitably be on interpreting existing international law in the context of cyber operations; for IHL, this means determining when cyber operations rise to the level of an armed conflict if unaccompanied by kinetic operations[264] and ascertaining how extant IHL principles and rules designed for a kinetic environment apply to cyber operations.[265]

Continuing the trend discussed *supra*, States have offered no granular expressions of *opinio juris* on the subject. On the contrary, elucidation of the particulars and details of the purported international regulation of cyber hostilities has been left almost entirely to non-State legal conjecture. The emergence of cyberspace seems to have captured the attention of IHL scholars, and those concerned with the use of force under *jus ad bellum,* to a greater extent than any other community of international legal commentators. A growing body of scholarship on a broad range of IHL cyber issues now exists, the most significant of which is the 2013 *Tallinn Manual on the International Law Applicable to Cyber Warfare.*[266]

Produced by an International Group of Experts (IGE) invited by the NATO Cooperative Cyber Defence Centre of Excellence (CCD COE), the *Tallinn Manual* identifies 95 customary international law rules of *jus ad bellum* and IHL and includes an extensive commentary that captures majority and minority viewpoints on their interpretation.[267] The experts included academics, former senior military lawyers, and former NGO legal advisors, as well as non-voting observers from the ICRC, U.S.

260. U.N. Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, Rep., transmitted by the Secretary-General, para. 19, U.N. Doc. A/68/98 (June 24, 2013). The experts came from Argentina, Australia, Belarus, Canada, China, Egypt, Estonia, France, Germany, India, Indonesia, Japan, the Russian Federation, the United Kingdom, and the United States.

261. The ICRC has taken this view, as did the *Tallinn Manual* International Group of Experts. *ICRC Challenges*, *supra* note 35, at 36–38; TALLINN MANUAL r. 22.

262. *See, e.g.*, Koh, American Society Remarks, *supra* note 144 (stating that international law applies to cyberspace). The Netherlands has likewise acknowledged that IHL applies in cyberspace. GOV'T OF THE NETH., GOVERNMENT RESPONSE TO THE AIV/CAVV REPORT ON CYBER WARFARE 5 (2012).

263. Mark A. Kochuk, *Symposium Review: Is There A Need for International Cyber Warfare Treaties?*, N. C. J. INT'L & COM. REG. BLOG (Feb. 13, 2014), http://blogs.law.unc.edu/ncilj/2014/02/13/symposium-review-is-there-a-need-for-international-cyber-warfare-treaties/.

264. JEREMY A. RABKIN & ARIEL RABKIN, HOOVER INST. STANFORD UNIV., TO CONFRONT CYBER THREATS, WE MUST RETHINK THE LAW OF ARMED CONFLICT 3–6 (2012), *available at* http://www.hoover.org/sites/default/files/uploads/inline/docs/EmergingThreats_Rabkin.pdf.

265. *Id.* at 6.

266. *See generally* TALLINN MANUAL. The authors were both members of the International Group of Experts that produced the *Manual.*

267. *See generally id.*

Cyber Command, and NATO.[268] While the process relied upon the logistical and financial support of the CCD COE, the manual itself was not a NATO product.[269] Its rules reflect only the views of the IGE, the members of which were all participating in their personal capacity.[270] On many topics of relevance to cyber warfare, the *Tallinn Manual* provides the most extensive and thorough legal analysis currently available.[271]

The *Tallinn Manual* has been cited widely in academic literature and at conferences.[272] Anecdotally, State reactions to it have been largely positive.[273] But no State has commented on the *Manual*'s conclusions in any comprehensive or definitive manner, nor has any State or group of States produced an analogous or competing product. And although the vast majority of the *Tallinn Manual*'s statements of law and commentary appear consistent with what little is known of State views on the application of IHL to cyber warfare, actual State expressions of *opinio juris* on the topics it addresses remain exceedingly vague.[274] For instance, shortly before publication, former State Department Legal Adviser Harold Koh delivered remarks on the applicability of international law to cyber operations.[275] They included a firm commitment to apply existing IHL to situations of armed conflict involving cyber activities.[276] But Koh failed to stake out clear or comprehensive positions with respect to most of the thorny legal issues identified in the *Tallinn Manual*.[277] The remarks drew attention since they were the first foray into the subject,[278] but they did little more than state the obvious.

There are, of course, colorable reasons for State reticence to set forth views on how IHL applies to cyber operations. To begin with, legal ambiguity may benefit States by affording them greater leeway to conduct and respond to cyber operations during an armed conflict.[279] Moreover, at this nascent stage in the development of

---

268. *Id.* Int'l Grp. of Experts.

269. *Id.* intro.

270. *Id.*

271. *See* Liis Vihul & Michael N. Schmitt, *The Tallinn Manual on Cyber Warfare–A First Tool for Legal Practitioners*, FIFTEENEIGHTYFOUR (Nov. 13, 2013), http://www.cambridgeblog.org/2013/11/the-tallinn-manual-on-cyber-warfare-a-first-tool-for-legal-practitioners-michael-schmitt-liis-vihul-nato/ [hereinafter Vihul & Schmitt, *First Tool for Legal Practitioners*] (recognizing the *Tallinn Manual* as the first detailed look at the law applicable to hostile cyber operations).

272. *See, e.g.*, the forum on the *Tallinn Manual*, *in* 15 Y.B. INT'L HUMAN. L. 3–58 (2012); Dieter Fleck, *Searching for International Rules Applicable to Cyber Warfare—A Critical First Assessment of the New* Tallinn Manual, 18 J. CONFLICT AND SECURITY L. 331 (2013).

273. Vihul & Schmitt, *First Tool for Legal Practitioners*, *supra* note 271.

274. *See generally* Koh, American Society Remarks, *supra* note 144 (discussing the U.S. Government's views on international law and cyber warfare).

275. *Id.*

276. *Id.*

277. *See generally* Michael N. Schmitt, *International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed*, 54 HARV. INT'L L.J. ONLINE 13, 15 (2012) [hereinafter Schmitt, *Speech and Manual Juxtaposed*] (providing "analytical granularity as to the legal basis for the positions proffered in the Koh Speech").

278. Ellen Nakashima, *Cyberattacks Could Trigger Self-Defense Rule, U.S. Official Says*, WASH. POST, Sept. 18, 2012, www.washingtonpost.com/world/national-security/us-official-says-cyberattacks-can-trigger-self-defense-rule/2012/09/18/c2246c1a-0202-11e2-b260-32f4a8db9b7e_story.html.

279. *See* Schmitt, *Rewired Warfare*, *supra* note 25, at 2, 4–7 (explaining that the permissive approach to applying IHL to cyber operations allows for a wider range of cyber operations against the civilian

cyber capabilities and threats, States may be conflicted as to the optimal position to take when interpreting existing law.[280] To illustrate, the United States is especially vulnerable to cyber operations due to the pervasive reliance of its armed forces on computers and computer networks, as well as the dependency of its civilian activities on cyber activities and infrastructure.[281] Yet, the country's armed forces also wield impressive cyber capabilities, as exemplified by the establishment of U.S. Cyber Command and its service components, which it can bring to bear on enemy forces.[282] The United States resultantly finds itself on the horns of a dilemma. A normatively permissive regime would place its military operations and civilian population at risk, but empower it to conduct aggressive cyber activities; a restrictive regime would confine its military options, but likewise limit the enemy's ability to exploit its cyber vulnerabilities or target its civilian population. Justified or not, the hesitancy of States to offer expressions of *opinio juris* on the law of cyber warfare has become palpable.

While States may not be prepared to comment expansively or with any degree of precision on how they believe IHL governs cyber operations, a number of key topics are plainly ripe for expressions of *opinio juris*. With debate over these topics in the academy and the NGO community maturing, States risk forfeiting the opportunity to shape the future legal environment of this "fifth domain" of warfare.[283] A sampling of four of the more contentious topics illustrates the importance of proactively engaging in their normative development.

First, the threshold question regarding the applicability of any IHL principle or rule is always whether a state of armed conflict exists, and, if so, whether that conflict is international or non-international in character.[284] Should an armed conflict not exist, human rights and domestic law will govern any forceful cyber operations that are mounted, not IHL.[285] These latter bodies of law do not countenance "attacks" (a term discussed *infra*) based on the status of the target (e.g., combatant, civilian direct participant in hostilities, military objective); there is accordingly no "belligerent immunity" for attacking lawful targets, as there would be during an armed conflict.[286] Therefore, absent an armed conflict, cyber operations likely to cause direct or indirect physical harm may only lawfully be launched in self-defense, defense of

---

population).

280. *See id.* at 2–3 (explaining the three different approaches used in interpreting how to apply IHL to cyber operations: permissive, restrictive, and the *Tallinn Manual*'s new approach).

281. Michael Assante, *America's Critical Infrastructure Is Vulnerable to Cyber Attacks*, FORBES (Sept. 11, 2014), http://www.forbes.com/sites/realspin/2014/11/11/americas-critical-infrastructure-is-vulnerable-to-cyber-attacks/.

282. Schmitt, *Rewired Warfare*, *supra* note 25, at 2.

283. *See* DEP'T OF DEF., QUADRENNIAL DEFENSE REVIEW REPORT 37 (2010), *available at* http://www.defense. gov/qdr/qdr%20as%20of%2026jan10%200700.pdf (listing cyberspace as a relevant domain for the DoD along with "land, sea, air, and space").

284. *See* Michael N. Schmitt, *Classification of Cyber Conflict*, 89 INT'L L. STUD. 233, 233 (2013) [hereinafter Schmitt, *Classification*] (stating that classifying a conflict as either international or non-international "is always the first step" in ILH analysis).

285. *See id.* at 236–39 (describing the ways in which the Geneva Conventions apply to armed conflicts).

286. Michael N. Schmitt, *International Law and Cyberwar: A Response to the Ethics of Cyberweapons*, ETHICS & INT'L AFF. (Feb. 10, 2014), http://www.ethicsandinternationalaffairs.org/2014/international-law-and-cyberwar-a-response-to-the-ethics-of-cyberweapons/.

others, or other situations allowing the use of force; in other words, cyber operations may be conducted only pursuant to a "law enforcement" legal regime.[287]

Of course, to the extent that kinetic hostilities qualify a conflict as international or non-international, IHL applicable in each of these two forms of armed conflict would apply to associated cyber operations.[288] The problematic question is instead whether a cyber exchange that includes no kinetic component can qualify as armed conflict, thereby opening the door to IHL. International armed conflict requires that there be "hostilities" between two or more States.[289] Although there are differences of opinion as to the requisite level of violence necessary to qualify a situation as an IAC,[290] there is general consensus that the threshold is low.[291] The question is how low. Must there be physical consequences such as damage or injury? If so, how much? In this respect, the IGE was divided as to whether the damage to Iranian centrifuges during the Stuxnet operations crossed the armed conflict line, assuming, of course, that other States were behind the operation.[292] There is evidently ample room for States to begin the process of developing the threshold vis-à-vis cyber operations.

Characterization of a situation as a NIAC, that is, conflict between a State and an organized armed group, or between two or more organized armed groups, is even more challenging in the cyber context.[293] Like IAC, once a situation qualifies as a NIAC, any cyber operations occurring as an element of that conflict will be governed by IHL.[294] A purely cyber exchange would be assessed against the two requirements for a NIAC articulated in the *Tadić* judgment by the ICTY for kinetic conflict.[295] There the tribunal held that the hostilities in question must have reached a particular level of intensity such that they can be distinguished from mere civil disturbances, riots, and the like, and they must involve an organized armed group.[296]

This test raises the question of whether a cyber campaign can qualify as sufficiently intense to satisfy the first criterion. Is the issue simply one of consequences, such that only cyber operations that, for example, result in widespread destruction or death qualify? Or does intensity refer to operations of a particular nature, like those that are violent in nature and occur openly? And may a group that

---

287. Eighth U.N. Congress on the Prevention of Crime and the Treatment of Offenders, Havana, Aug. 27–Sept. 7, 1990, Rep. of the Secretariat, at 108–14, U.N. Doc. A/CONF.144/28/Rev.1 (1991) (describing when law enforcement officials may properly use force).

288. Schmitt, *Classification*, *supra* note 284, at 239–40.

289. The accepted articulation of an IAC is found in Common Article 2 of the four 1949 Geneva Conventions. *See supra* note 9.

290. *See* TALLINN MANUAL r. 22 cmt. 12 (noting that "controversy exists as to the threshold of the requisite violence").

291. *Id.*

292. *Id.* r. 22 cmt. 14.

293. The accepted articulation of a NIAC is found in Common Article 3 of the four 1949 Geneva Conventions. *See supra* note 9.

294. *See* Herbert Lin, *Cyber Conflict and International Humanitarian Law*, 94 INT'L REV. RED CROSS 515 (2012) (commenting that non-state actors' relevance increases in cyber conflict and discussing what should be done about cyber conflict in international law).

295. *See* Schmitt, *Classification*, *supra* note 284, at 245 (discussing that the ICTY stated that a NIAC had to be "organized" and "armed").

296. Prosecutor v. Tadić, Case No. IT-94-1-I, Decision on Defence Motion for Interlocutory Appeal on Jurisdiction, para. 70 (Int'l Crim. Trib. for the Former Yugoslavia Oct. 2, 1995).

is organized entirely online qualify as an organized armed group for the purpose of meeting the second criterion? It is common for members of online groups to not know each other.[297] May such a group be "organized" in the IHL sense?[298] How would it enforce discipline, a commonly accepted requirement for organization?[299] What if, as happened in the Estonia and Georgia cases, individuals throughout a country, and even abroad, began conducting cyber operations against the State based solely on online calls to do so?[300] Should such operations be considered a NIAC if they meet the intensity requirement? The need for States to express *opinio juris* on the characterization of cyber conflicts is acute since the existence of an armed conflict, or not, will shape the response options available to them when facing hostile cyber operations.[301]

Equally important is the second topic, the meaning of the term "attack" in the cyber context.[302] Many IHL rules that extend protection to particular persons and objects, or that dictate how certain military operations may be conducted, are framed in terms of "attacks."[303] For instance, it is prohibited to directly "attack" civilians or civilian objects.[304] It is also prohibited to conduct an "attack" against a valid military objective if the expected collateral damage would be excessive to the anticipated military advantage of the operation.[305] The question in the cyber context is whether these rules are applicable to a particular cyber operation such that, for example, it may not be directed at civilian cyber infrastructure, or is prohibited because the effect of the operation on civilian systems is likely to be excessive. They will apply if the cyber operation qualifies as an attack; they will not if the operation does not so qualify.

It is widely agreed that a cyber operation that directly or indirectly causes physical damage or injury to persons during an armed conflict qualifies as an attack and is therefore subject to the various IHL principles and rules governing such operations.[306] General consensus also exists that cyber operations resulting in mere inconvenience or slight disruption to cyber activities are not attacks in the IHL sense.[307] The unresolved question is: "When do cyber operations falling between

297. Schmitt, *Classification*, *supra* note 284, at 246.

298. *Id.*

299. *Id.*

300. *Compare* TALLINN MANUAL r. 23 cmt. 5 (discussing "the calls that appeared on the Internet for riots by the Russian minority in Estonia in 2007"), *with* Dancho Danchev, *Coordinated Russia vs Georgia Cyber Attack in Progress*, ZDNET (Aug. 11, 2008) http://www.zdnet.com/blog/security/coordinated-russia-vs-georgia-cyber-attack-in-progress/1670 (discussing "self-mobilization of the local Internet users by spreading '*For our motherland, brothers!*' or '*Your country is calling you!*' hacktivist messages across web forums").

301. Schmitt, *Classification*, *supra* note 284, at 250 (explaining the role of *opinio juris* in regards to cyber operations).

302. *See id.* at 239–44 (discussing the difficulties of classifying cyber operations as an attack).

303. *See id.* (discussing attacks as defined by the ICRC).

304. ICRC, *From Law to Action*, *supra* note 37, at 62, 65.

305. *See id.* at 62 (condemning the massive killing of civilians in armed attacks and urging compliance with the principles of IHL).

306. *See* TALLINN MANUAL r. 30 ("A cyber attack is a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects.").

307. *Id.* r. 94.

these two ends of the continuum amount to attacks?" The IGE struggled with this issue throughout the three years of the *Tallinn Manual* project.[308] Eventually, the majority agreed that a cyber operation significantly affecting the "functionality" of cyber infrastructure is an attack.[309] This conclusion was not unanimous.[310] Moreover, there were differences of opinion within the majority. For example, the experts concerned disagreed on whether a cyber operation that required reloading the operating system or otherwise necessitated replacement of key data qualified.[311]

The issue of the qualification of cyber operations as attacks lies at the heart of IHL's application in the cyber context. A narrow interpretation of the notion would open the door to highly disruptive cyber operations directed against the civilian population and other protected persons and objects.[312] Consider the impact of non-destructive but widespread cyber operations targeting the enemy's economy or governmental functions.[313] The severity of the consequences would far outstrip those of many kinetic operations.[314] It would seem incongruent to interpret IHL to allow the former, but not the latter. On the other hand, a broad interpretation of attack could limit military operations well beyond what is currently acceptable. Psychological operations directed at the civilian population, for example, have long been conducted by militaries.[315] Should such operations now be prohibited merely because the medium used is cyber in nature? Unless States begin to address the issue of where the line between a mere operation and one that qualifies as an attack lies, the issue will be addressed for them by non-State actors in a manner that may prove difficult to reverse.

A third area of uncertainty involves who may be attacked by cyber means.[316] Objectively, the universe of lawful human targets is well settled: combatants, members of organized armed groups, and civilians who are directly participating in hostilities.[317] Practical application, however, remains muddled. Recall the debate over the purported continuous combat function criterion for targeting members of an

---

308. Schmitt, *Rewired Warfare*, *supra* note 25, at 9.

309. TALLINN MANUAL r. 30 cmt. 10.

310. Schmitt, *Rewired Warfare*, *supra* note 25, at 9–10

311. *Id.*; *see also* Cordula Droege, *Get Off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians*, 94 INT'L REV. RED CROSS 533, 557–59 (2012) (analyzing the functionality test in the *Tallinn Manual*).

312. *See* Droege, *supra* note 311, at 538–40 (discussing cyber operations' possible effects on civilian infrastructure).

313. *See, e.g.*, TALLINN MANUAL intro. (explaining that the United Kingdom considers cyber attacks to be Tier One threat to national security and "one of the most serious national security, public safety, and economic challenges we face as a nation").

314. *Cf. id.* (highlighting the seriousness with which the United Kingdom takes such threats).

315. *See id.* r. 11 cmt. 9(h) ("[I]nternational law does not prohibit propaganda, psychological operations, espionage, or mere economic pressure *per se*. Therefore, acts falling into these and other such categories are presumptively legal . . . ."); DEP'T OF THE ARMY, FIELD MANUAL 3-05.30: PSYCHOLOGICAL OPERATIONS 1-7 (discussing psychological operations of the U.S. forces in Romania during World War I).

316. *See* TALLINN MANUAL intro. ("One of the challenges States face in the cyber environment is that the scope and manner of international law's applicability to cyber operations, whether in offence or defence, has remained unsettled since their advent."); Droege, *supra* note 311, at 540–41, 553–56 (discussing various scholarly authors' arguments on the question of who can be attacked by cyber warfare).

317. TALLINN MANUAL r. 34 cmts. 1–9.

organized armed group.[318] In contemporary conflicts, organized armed groups often rely heavily on cyber assets for, *inter alia*, communications, logistics functions, intelligence gathering, and psychological operations.[319] To what extent are members of the group who maintain and operate cyber infrastructure for these purposes engaging in a continuous combat function and, if they are not, should they be immune from direct attack on that basis? Assuming, solely for the purpose of analysis, that such individuals are immune from direct attack, any expected incidental harm to them during an attack on other members of the group would have to be factored into the proportionality calculation and would be a consideration in determining the precautions that would be required in conducting the attack.[320] On the other hand, if their role does qualify as a continuous combat function, or if no continuous combat function criterion exists as a matter of law, the individuals concerned could lawfully be attacked directly and any indirect harm they suffered during an attack on other persons or objects would have no proportionality or precautions in attack implications.[321]

Similar interpretive dilemmas stand in the way of clear application of the direct participation by civilians in hostilities rule discussed *supra*. For instance, when does maintenance or operation of enemy cyber infrastructure by a civilian who is not a member of an organized armed group rise to the level of direct participation in hostilities? Is there a difference between maintenance of cyber infrastructure used by enemy forces for purposes unrelated to the conflict (e.g., at a military school) and maintenance of systems used to conduct cyber attacks? Does it matter if the cyber infrastructure is dual use (used for both military and civilian purposes) or used exclusively by the military? Is the creation of malware that is incidentally used by enemy forces an act of direct participation? Must the malware be intended for enemy use? Or must it be created for a particular enemy cyber operation? Is passive cyber defense of enemy systems an act of direct participation such that contractors who perform the task lose their immunity from attack? State expressions of *opinio juris* as to the proper criteria to employ in assessing these and many other activities would contribute measurably to consistent application of the rule in the cyber context and help shape it in a fashion that advances both military necessity and humanitarian concerns.

A final topic illustrating the need for expressions of *opinio juris* involves the requirement to take care to minimize harm to civilians and civilian objects when conducting an attack.[322] Assuming 1) IHL applies because the situation is one of armed conflict, 2) the cyber operation is an attack and therefore subject to the IHL rules thereon, and 3) the individual or object against which the cyber attack is directed qualifies as a lawful target, an attacker must still take all feasible measures to limit incidental harm to civilians and civilian objects.[323] In particular, the attacker

318. *See supra* notes 89–97 and accompanying text.

319. TALLINN MANUAL r. 6 cmt. 8; r. 22 cmts. 6–7; r. 31 cmt. 5.

320. *See* DPH GUIDANCE, *supra* note 51, at 1024 (determining that "a direct attack against the [civilian driver of an ammunitions truck] would have to take the probable death of the civilian driver into account in the proportionality assessment").

321. *Id.* at 994 n.6.

322. AP I art. 57; 1 CUSTOMARY IHL STUDY r. 15.

323. *See* AP I art. 57(2)(a)–(b) (requiring that those conducting military operations "[t]ake all feasible precautions in the choice of means and methods of attack with a view to avoiding, and in any event to

must engage in reasonable steps to verify the target, endeavor to employ methods or means of attack that minimize harm to civilians or civilian objects without sacrificing military advantage, and select targets the attack upon which will minimize civilian harm while achieving the attacker's sought after effect.[324]

Application of the precautions in attack rule is problematic in the cyber context, in part because military commanders and operational planners generally lack the depth of understanding of cyber operations that they have of kinetic attacks.[325] Therefore, when cyber operations are a component of an operation, it is more difficult for them to understand how best to verify the status of a potential cyber target as a lawful military objective, identify the various options available with respect to cyber weapons and potential cyber targets, and assess the collateral effects of the proposed cyber operations.[326] Additionally, the complexity of cyber networking and the difficulty of assessing bleed over effects complicate application of the obligation to take precautions in attack.[327] As an example, it will often be difficult to gauge likely collateral damage when attacking dual use cyber infrastructure or cyber infrastructure networked into civilian systems.[328] Without fully understanding the scope of potential collateral damage, identifying and assessing those measures available to avoid potential collateral damage becomes problematic.

---

minimizing, incidental loss of civilian life, injury to civilians and damage to civilian objects; [r]efrain from deciding to launch any attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated;" and cancel or suspend an attack "if it becomes apparent that the . . . attack may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated . . . .").

324. *See generally id.*

325. *See* Schmitt, *Speech and Manual Juxtaposed*, *supra* note 277, at 25–31 (explaining the difficulties of applying international humanitarian law principles, particularly proportionality, to cyber attacks).

326. For instance, an object that has both military and civilian purposes can be classified as "military," and, therefore, a proper target, even if the military use of the objective is only marginal. Droege, *supra* note 311, at 562–64. "The consequence of this would be that in some circumstances virtually all parts of the Internet might qualify as a military objective because they are all possible routes for the transmission of military information." *Id.* at 564. *See also* TALLINN MANUAL r. 39 cmt. 3 ("Cyber operations pose unique challenges in this regard. Consider a network that is being used for both military and civilian purposes. It may be impossible to know over which part of the network military transmissions, as distinct from civilian ones, will pass. In such cases, the entire network (or at least those aspects in which transmission is reasonably likely) qualifies as a military objective.").

327. *See* Droege, *supra* note 311, at 564 (discussing the difficulties in assessing whether cyber networks are civilian or military); TALLINN MANUAL r. 52 cmt. 6 ("Given the complexity of cyber operations, the high probability of affecting civilian systems, and the sometimes limited understanding of their nature and effects on the part of those charged with approving cyber operations, mission planners should, where feasible, have technical experts available to assist them in determining whether appropriate precautionary measures have been taken.").

328. *See, e.g.*, *id.* at 539 ("[I]t is to a large extent impossible to differentiate between purely civilian and purely military computer infrastructure. . . . [T]his poses a serious challenge to one of the cardinal principles of IHL, namely the principle of distinction between military and civilian objects. Moreover, even if military and civilian computers or computer systems are not entirely one and the same, interconnectivity means that the effects of an attack on a military target may not be confined to this target. . . . [A]n attack on a military computer system may well also damage civilian computer systems, which, in turn, may be vital for some civilian services such as water or electricity supply or the transfer of assets.").

Perhaps the greatest obstacle to application of the rule is the fact that an attacker is only required to take "feasible" precautions in attack.[329] Feasibility is assessed on a case-by-case basis taking into account such factors as the target setting, the availability of other weapons, competing demands for ISR assets, and the intended effect of the operation.[330] Doing so in the kinetic environment is difficult; in light of the factors just mentioned,[331] assessing feasibility in the cyber environment will be even more so. As with the example, it is essential that States begin to shape expectations as to the requisite precautions in cyber attack. Inattention to this practical need risks the advent of requirements that may frustrate the achievement of legitimate military objectives.

The four examples are far from exhaustive. However they do illustrate the severity of risks that States will be assuming if the trend of refraining from offering clear expressions of *opinio juris* regarding IHL endures. The risks are particularly grave with respect to cyber operations because such operations are typically classified. Thus, there will often be no visible State practice from which to draw even inferences of *opinio juris*. As non-State actors engage in activities that take the place of State expressions of *opinio juris* in the development and interpretation of IHL cyber norms, they may well be operating on partial or faulty information as to actual State practice.

CONCLUSION

This has been an article about process, not substance. It is meant to be neither polemical nor Manichean. It offers no comment on any position that has been asserted by non-State actors or States with respect to the interpretation of extant IHL or its apparent evolutionary vector. Instead, we simply lament the fact that States, perhaps without even realizing they have been doing so, are ceding control over the content, interpretation, and development of IHL to others. Greater sensitivity on the part of States to the centrality of expressing *opinio juris* to law formation and interpretation appears merited.

The reluctance of States and their legal representatives to communicate and commit to clear views on IHL matters vitiates legal discourse, degrading the functioning and development of a critical aspect of the international legal system. Scholars, commentators, advocates, judges, and even States' own diplomats and legal advisors are by now accustomed to resorting to speculation to resolve ambiguity concerning any number of State views on IHL. Paradoxically, in the absence of State views, such speculation can become, over time, the law. Unless the trend is reversed,

329. *See* AP I art. 57(2)(a)(ii) ("Those who plan or decide upon an attack shall . . . [t]ake all *feasible* precautions in the choice of means and methods of attack with a view to avoiding, and in any event to minimizing, incidental loss of civilian life, injury to civilians and damage to civilian objects . . . ." (emphasis added)).

330. *See* TALLINN MANUAL r. 53 cmt. 5 ("[F]easible precautions might include gathering intelligence on the network through mapping or other processes in order to allow those responsible reasonably to determine the attack's likely effects, particularly on the civilian population or civilian objects. There is no obligation to take measures that are not feasible.").

331. *See* 1 CUSTOMARY IHL STUDY r. 22 (discussing the fact that "small and densely populated countries . . . would find it difficult to separate civilians and civilian objects from military objectives and that even large countries would find such separation difficult or impossible to arrange in many cases").

States stand in peril of losing sway over debates that may significantly and adversely impact their freedom of action on the battlefield, or even place their civilian population at increased risk.

In our view, a number of important and emerging legal issues related to cyber operations during armed conflict are now ripe for expressions of *opinio juris* by States, including the United States. This should be unsurprising since not one of the existing IHL principle or rules, treaty or customary, was crafted or crystallized with cyber operations in mind. Accordingly, State expressions of *opinio juris* take on added importance as cyber capabilities are developed and fielded.

Whether to announce doctrinal details and clarifications, preserve flexibility through confirmation of ambiguity, or simply reject or confirm the existence of particular norms, such expression of *opinio juris* manage important State legal and operational interests. Therefore, State legal agencies and agents, particularly Ministries and Departments of Defense, must be equipped, organized, and empowered to participate actively in the interpretation and development of IHL. States, and specially affected States in particular, must make responses to emerging IHL scholarship, investigations and jurisprudence a regular facet of their *opinio juris*. Reinvigorating *opinio juris* would do more than satisfy international law sovereigntists. It would foster the restoration of the pluralistic IHL dialogue that formerly tested, updated, and enriched the balance between military necessity and humanitarian considerations that necessarily underpins IHL. In no field is such activism in greater demand than the international regulation of cyber warfare.

Evidentiary Issues in International Disputes Related to State Responsibility for Cyber Operations

MARCO ROSCINI*

SUMMARY

* Reader in International Law, University of Westminster. I am grateful to Simon Olleson for his useful comments on a previous version of this article and to Andraz Kastelic for his research assistance. All errors and omissions remain my sole responsibility. The article is based on developments as of June 2014 and all websites were last visited during that time.

INTRODUCTION

Evidentiary problems in inter-state litigation, particularly in relation to the attribution of certain unlawful conduct, are not peculiar to cyber operations.[1] Well before the cyber age, the International Court of Justice (ICJ) in the *Nicaragua v. United States* judgment conceded that "the problem is . . . not . . . the legal process of imputing the act to a particular State . . . but the prior process of tracing material proof of the identity of the perpetrator."[2] As the United States declared in the views on information security that it submitted to the U.N. Secretary-General, then, the ambiguities of cyberspace "simply reflect the challenges . . . that already exists [sic] in many contexts."[3] It is undeniable, however, that these challenges are particularly evident in the cyber context, where identifying who is behind a cyber operation presents significant technical problems.[4] As has been effectively observed, "the Internet is one big masquerade ball. You can hide behind aliases, you can hide behind proxy servers, and you can surreptitiously enslave other computers . . . to do your dirty work."[5]

One needs only look at the three most famous cases of cyber attacks against States allegedly launched by other States to realize how thorny the problem of evidence in relation to cyber operations is.[6] It has been claimed, in particular, that the Russian Federation was behind both the 2007 Distributed Denial of Service (DDoS) attacks against Estonia and the 2008 cyber attacks against Georgia.[7] These

---

1. TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE glossary (Michael N. Schmitt ed., 2013) [hereinafter TALLINN MANUAL] (defining cyber operations as "the employment of cyber capabilities with the primary purpose of achieving objectives in or by the use of cyberspace"). Cyber operations include cyber attacks and cyber exploitation. Cyber attacks are those cyber operations, whether in offense or in defense, intended to alter, delete, corrupt, or deny access to computer data or software for the purposes of (a) propaganda or deception; (b) partly or totally disrupting the functioning of the targeted computer, computer system, or network with any related computer-operated physical infrastructure; and/or (c) producing physical damage extrinsic to the computer, computer system, or network. Cyber exploitation refers to those operations that access other computers, computer systems, or networks, without the authorization of their owners or exceeding the limits of the authorization in order to obtain information, but without affecting the functionality of the accessed system or amending/deleting the data resident therein. For a discussion of these definitions, see MARCO ROSCINI, CYBER OPERATIONS AND THE USE OF FORCE IN INTERNATIONAL LAW 10–18 (2014).

2. Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U. S.), Judgment, 1986 I.C.J. 14, para. 57 (June 27).

3. U.N. Secretary-General, *Developments in the Field of Information and Telecommunications in the Context of International Security: Rep. of the Secretary-General*, 18, U.N. Doc. A/66/152 (July 15, 2011) [hereinafter *Developments in the Field of Information and Telecommunications*].

4. *Cf.* FIREEYE, DIGITAL BREAD CRUMBS: SEVEN CLUES TO IDENTIFYING WHO'S BEHIND ADVANCED CYBER ATTACKS 4 (2014), *available at* https://www.fireeye.com/resources/pdfs/digital-bread-crumbs.pdf (describing the technical difficulty in pinning down the source of a cyber attack given that "[c]ybercriminals are experts at misdirection" even in the non-State actor context).

5. JOEL BRENNER, AMERICA THE VULNERABLE: INSIDE THE NEW THREAT MATRIX OF DIGITAL ESPIONAGE, CRIME, AND WARFARE 32 (2011); *see also Developments in the Field of Information and Telecommunications*, *supra* note 3 ("The lack of timely, high-confidence attribution and the possibility of 'spoofing' can create uncertainty and confusion for Governments, thus increasing the potential for crisis instability, misdirected responses and loss of escalation control during major cyberincidents.").

6. The three most famous cases of cyber attacks are the Distributed Denial of Services (DDoS) attacks against Estonia in 2007, the cyber attacks against Georgia in 2008, and the Stuxnet attacks against Iran discovered in 2012.

7. Ian Traynor, *Russia Accused of Unleashing Cyberwar to Disable Estonia,* THE GUARDIAN, May 16, 2007, http://www.theguardian.com/world/2007/may/17/topstories3.russia; Jon Swaine, *Georgia: Russia*

allegations were based on the following facts. In the Estonian case, the hackers claimed to be Russian, the tools to hack and deface were contained in Russian websites and chatrooms, and the attacks peaked on May 9 (the day Russia celebrates Victory in Europe Day in the Second World War).[8] Furthermore, although the botnets included computers based in several countries, it seems that at least certain attacks originated from Russian IP addresses, including those of State institutions.[9] According to the Estonian Defense Minister, the attacks were "unusually well-coordinated and required resources unavailable to common people."[10] The DDoS attacks also took place against the backdrop of the removal of a Russian war memorial from Tallinn's city center.[11] Finally, Russia did not cooperate with Estonia in tracking down those responsible, and the Russian Supreme Procurature rejected a request for bilateral investigation under the Mutual Legal Assistance Treaty between the two countries.[12]

The cyber attacks against Georgia started immediately before and continued throughout the armed conflict between the Caucasian State and the Russian Federation in August 2008.[13] It seems that the Russian hacker community was involved in the cyber attacks and that coordination "took place mainly in the Russian language" and in Russian or Russian-related fora.[14] As in the Estonian case, some commentators claimed that the level of coordination and preparation suggested governmental support for the cyber attacks.[15] Finally, IP addresses belonging to

---

'Conducting Cyber War,' THE TELEGRAPH, Aug. 11, 2008, http://www.telegraph.co.uk/news/worldnews/europe/georgia/2539157/Georgia-Russia-conducting-cyber-war.html. For a discussion of denial of service attacks, see ROSCINI, *supra* note 1, at 18. "Denial of Service (DoS) attacks, of which 'flood attacks' are an example . . . do not normally penetrate into the system but aim to inundate the target with excessive calls, messages, enquiries, or requests in order to overload it and force its shut down. Permanent DoS attacks are particularly serious attacks that damage the system and cause its replacement or reinstallation of hardware. When the DoS attack is carried out by a large number of computers organized in botnets, it is referred to as a DDoS attack." *Id.*

8. COMM. ON OFFENSIVE INFO. WARFARE, NAT'L RESEARCH COUNCIL, TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES 173 box 3.4 (William A. Owens, Kenneth W. Dam & Herbert S. Lin eds., 2009) [hereinafter U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES].

9. *Id.*

10. *Id.* (quoting Jaak Aaviksoo, Minister of Defense of Estonia, Strategic Impact of Cyber Attacks, Address before the Royal College of Defence Studies, *available at* www.irl.ee/en/articles/strategic-impact-of-cyber-attacks.

11. U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES.

12. Scott J. Shackelford, *From Nuclear War to Net War: Analogizing Cyber Attacks in International Law*, 27 BERKELEY J. INT'L L. 192, 208 (2009); *see also* Alexander Klimburg, *Mobilising Cyber Power*, 53 SURVIVAL: GLOBAL POL. & STRATEGY 41, 49–51 (2011) (describing Russia's recent support for cyber criminals in combating internal and external threats).

13. *See* John Markoff, *Before the Gunfire, Cyberattacks*, N.Y. TIMES, Aug. 13, 2008, http://www.nytimes.com/2008/08/13/technology/13cyber.html?_r=0 (describing the cyberattacks as "dress rehearsal" before the shooting began in the Russo-Georgian War).

14. ENEKEN TIKK ET AL., COOP. CYBER DEF. CTR. OF EXCELLENCE, INTERNATIONAL CYBER INCIDENTS: LEGAL CONSIDERATIONS 75 (2010), *available at* http://www.ccdcoe.org/publications/books/legalconsiderations.pdf.

15. *Id.*

Russian state-operated companies were used to launch the DDoS attacks.[16] Russia again denied any responsibility.[17]

The third case of alleged inter-state cyber operation, and possibly the most famous of the three, is that of Stuxnet. In 2012, an article published in *The New York Times* revealed that the United States, with Israel's support, had been engaging in a cyber campaign against Iran, codenamed "Olympic Games," to disrupt the Islamic Republic's nuclear program.[18] Stuxnet, in particular, was allegedly designed to affect the gas centrifuges at the Natanz uranium enrichment facility.[19] The Stuxnet incident was the first known use of malicious software designed to produce material damage by attacking the Supervisory Control and Data Acquisition (SCADA) system of a critical national infrastructure.[20] Unlike other malware, the worm did not limit itself to self-replication, but also contained a weaponized payload designed to give instructions to other programs.[21] The allegations against the United States and Israel were based on journalistic "interviews . . . with current and former American, European and Israeli officials" and other experts, whose names are not known.[22] In a recent interview, the former U.S. National Security Agency (NSA) contractor Edward Snowden also claimed that the NSA and Israel were behind Stuxnet.[23] Symantec's researchers suggested that Stuxnet's code included references to the 1979

16. *Id.*

17. *Id.*

18. David E. Sanger, *Obama Order Sped Up Wave of Cyberattacks Against Iran*, N.Y. TIMES, June 1, 2012, http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all&_r=1&.

19. William J. Broad, John Markoff, & David E. Sanger, *Israeli Test on Worm Called Crucial in Iran Nuclear Delay*, N.Y. TIMES, Jan. 15, 2011, http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?pagewanted=all. Stuxnet presumably infiltrated the Natanz system through laptops and USB drives—as, for security reasons, the system is not usually connected to the Internet—and had two components: one designed to force a change in the centrifuges' rotor speed, inducing excessive vibrations or distortions that would destroy the centrifuges, and one that recorded the normal operations of the plant and then sent them back to plant operators so to make it look as if everything were functioning normally. *See generally* HOLLY PORTEOUS, LIBRARY OF PARLIAMENT, THE STUXNET WORM: JUST ANOTHER COMPUTER ATTACK OR A GAME CHANGER? 1–2 (2010).

20. Dominic Storey, *Stuxnet–The First Worm of Many for SCADA?*, IT RESELLER (Dec. 2, 2010), http://www.itrportal.com/articles/2010/12/02/6262-stuxnet-the-first-worm-of-many-for; *see also* Thomas Rid, *Cyber War Will Not Take Place*, 35 J. STRATEGIC STUD. 5, 18–20 (2012) (describing Stuxnet's unique and innovative features).

21. Jeremy Richmond, Note, *Evolving Battlefields: Does Stuxnet Demonstrate a Need for Modifications to the Law of Armed Conflict?*, 35 FORDHAM INT'L L.J. 842, 849–50 (2012). Although the exact consequences of the incident are still the object of debate, the International Atomic Energy Agency (IAEA) reported that, in the period when Stuxnet was active, Iran stopped feeding uranium into a significant number of gas centrifuges at Natanz. *See* William J. Broad, *Report Suggests Problems with Iran's Nuclear Effort*, N.Y. TIMES, Nov. 23, 2010, http://www.nytimes.com/2010/11/24/world/middleeast/24nuke.html (describing Iran's various problems with its nuclear reactors while Stuxnet was operational, as well as international opinion as to whether Stuxnet caused those problems). It is still unclear, however, whether this was due to Stuxnet or to technical malfunctions inherent to the equipment used. *See* Ivanka Barzashka, *Are Cyber-Weapons Effective? Assessing Stuxnet's Impact on the Iranian Enrichment Programme*, 158 RUSI J. 48, 52 (2013) (proposing alternative explanations, including faulty machine parts, for the drop in centrifuge numbers).

22. Sanger, *supra* note 18.

23. *Edward Snowden Interview: The NSA and Its Willing Helpers,* SPIEGEL ONLINE (July 8, 2013), http://www.spiegel.de/international/world/interview-with-whistleblower-edward-snowden-on-global-spying-a-910006.html.

date of execution of a prominent Jewish Iranian businessman.[24] Other circumstantial evidence includes the fact that the worm primarily hit Iran and was specifically targeted at the Natanz nuclear facility, as the worm would activate itself only when it found the Siemens software used in that facility,[25] and the implication that the attack required resources normally unavailable to individual hackers, which is supported by evidence of the high sophistication of the attack, the use of several zero-day hacks, and the insider knowledge of the attacked system.[26] Israeli and U.S. officials have neither denied nor confirmed involvement in the operation: In response to a question about the attack on Iran, President Obama's chief strategist for combating weapons of mass destruction, Gary Samore, sardonically pointed out, "I'm glad to hear they are having troubles with their centrifuge machines, and the U.S. and its allies are doing everything we can to make it more complicated."[27] According to *The Daily Telegraph*, a video that was played at a retirement party for Israel Defense Forces (IDF) chief of general staff Gabi Ashkenazi included references to Stuxnet as one of Ashkenazi's operational successes.[28]

Apart from the above well-known cyber attacks, allegations of state involvement have also been made in relation to other cyber operations, including cyber exploitation activities. The U.S. Department of Defense's 2013 Report to Congress, for instance, claims that some of the 2012 cyber intrusions into U.S. government computers "appear to be attributable directly to the Chinese government and military," although it is not entirely clear on what grounds.[29] According to the controversial Mandiant Report, "the sheer number of [hacking group] APT1 IP addresses concentrated in these Shanghai ranges, coupled with Simplified Chinese keyboard layout settings on APT1's attack systems, betrays the true location and language of the operators."[30] The Report concludes that "APT1 is likely government-sponsored and one of the most persistent of China's cyber threat actors."[31] According to the Chinese Defense Ministry, however, "the report lacked 'technical proof'" linking the IP addresses used by ATP1 to a military unit of the People's Liberation Army (PLA), as the attacks employed hijacked addresses.[32] In

24. NICOLAS FALLIERE, LIAM O. MURCHU & ERIC CHIEN, SYMANTEC, W32.STUXNET DOSSIER, VERSION 1.4, at 18 (2011), *available at* http://www.symantec.com/content/en/us/enterprise/media/security_response/ whitepapers/w32_stuxnet_dossier.pdf.

25. *See* Barzashka, *supra* note 21, at 50 (explaining that "more than 60 per cent of all infected IP . . . addresses were in Iran, and almost 70 per cent of these had Siemens software installed").

26. *See* Rid, *supra* note 20, at 19 (explaining that "[t]he resources and investment that went into Stuxnet could only be mustered by a cyber superpower . . . .") (internal quotation marks omitted).

27. Broad, Markoff & Sanger, *supra* note 19.

28. Christopher Williams, *Israel Video Shows Stuxnet as One of Its Successes*, TELEGRAPH, Feb. 15 2011, http://www.telegraph.co.uk/news/worldnews/middleeast/israel/8326387/Israel-video-shows-Stuxnet-as-one-of-its-successes.html.

29. U.S. DEP'T OF DEF., ANNUAL REPORT TO CONGRESS: MILITARY AND SECURITY DEVELOPMENTS INVOLVING THE PEOPLE'S REPUBLIC OF CHINA 2013, at 36 (2013), *available at* http://www.defense.gov/pubs/ 2013_china_report_final.pdf.

30. MANDIANT, APT1: EXPOSING ONE OF CHINA'S CYBER ESPIONAGE UNITS 39 (2013) [hereinafter MANDIANT, APT1], *available at* http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.

31. *Id.* at 2.

32. *China Condemns Hacking Report by US Firm Mandiant*, BBC (Feb. 20, 2013), http://www.bbc.co.uk/news/world-us-canada-21515259.

May 2014, the U.S. Department of Justice eventually brought charges against five members of the PLA for hacking into the computers of six organizations in western Pennsylvania and elsewhere in the United States to steal trade secrets, without providing much supporting evidence (if any at all) of the involvement of the defendants.[33]

In spite of the obvious crucial importance of evidentiary issues, works on inter-state cyber operations, both above and below the level of use of force, have so far focused on whether such operations are consistent with primary norms of international law and on the remedies available to the victim State under the *jus ad bellum* and the law of state responsibility. Thus, studies of these operations have almost entirely neglected a discussion of the evidence the victim State needs to produce to demonstrate, either before a judicial body or elsewhere, that an unlawful cyber operation has been conducted against it and that the attack is attributable to another State.[34] The first edition of the *Tallinn Manual on the International Law Applicable to Cyber Warfare* also does not discuss in depth evidentiary issues in the cyber context: The only references to evidence are contained in Rules 7 and 8.[35] The present article aims to fill this gap. It will start with a brief account of the international law of evidence and will then discuss who has the burden of proof in relation to claims seeking remedies (including reparation) for damage caused by cyber operations. It will then analyze the standard of proof required in the cyber context. Finally, the possible methods of proof will be examined, distinguishing between those that are admissible and those that are inadmissible. The present article only deals with international disputes between States and will not discuss evidentiary issues in relation to cyber crime before domestic courts. It also does not look at evidence before international criminal tribunals, as the focus is on state responsibility for cyber operations and not on the criminal responsibility of individuals.[36]

---

33. *See* Indictment at 29–35, United States v. Wang Dong, No. 14-118 (W.D. Pa., May 1, 2014), *available at* http://www.justice.gov/iso/opa/resources/5122014519132358461949.pdf (laying out the facts and evidence related to the five defendants' overt cyber attacks).

34. *See generally* Robin Geiß & Henning Lahmann, *Freedom and Security in Cyberspace: Shifting the Focus away from Military Responses Towards Non-Forcible Countermeasures and Collective Threat-Prevention*, *in* PEACETIME REGIME FOR STATE ACTIVITIES IN CYBERSPACE: INTERNATIONAL LAW, INTERNATIONAL RELATIONS AND DIPLOMACY 621 (Katharina Ziolkowski ed., 2013) [hereinafter PEACETIME REGIME FOR STATE ACTIVITIES IN CYBERSPACE] (explaining the problems of attribution of responsibility for cyber attacks in the context of self-defense considerations); *see also* Scott J. Shackelford & Richard B. Andres, *State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem*, 42 GEO. J. INT'L L. 971, 984–93 (2011) (positing standards of evidence and describing the problems with evidence and attribution of cyber attacks to different sovereigns). In the context of law enforcement, the Council of Europe and European Union have drafted an Electronic Evidence Guide for cyber crime. CYBERCRIME@IPA JOINT PROJECT OF THE COUNCIL OF EUROPE AND THE EUROPEAN UNION, *Electronic Evidence Guide: A Basic Guide for Police Officers, Prosecutors, and Judges* (Mar. 18, 2013), *available at*, http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Electronic%20Evidence%20Guide/default_en.asp.

35. TALLINN MANUAL r. 7–8.

36. The statutes and rules of international criminal tribunals provide for specific evidentiary rules. Rüdiger Wolfrum, *International Courts and Tribunals, Evidence*, *in* 5 THE MAX PLANCK ENCYCLOPEDIA OF PUBLIC INTERNATIONAL LAW 552, 567–69 (Rüdiger Wolfrum ed., 2012).

I. THE INTERNATIONAL LAW OF EVIDENCE

"Evidence" is "information . . . with the view of establishing or disproving alleged facts."[37] It is different from proof in that "'proof' is the result or effect of evidence, while 'evidence' is the medium or means by which a fact is proved or disproved."[38] Evidence is normally required to provide proof of both the objective (be it an act or omission) and subjective elements of an internationally wrongful act, i.e., its attribution to a State.[39] A State invoking self-defense against cyber attacks, for instance, will have to produce evidence that demonstrates (a) that the cyber attack actually occurred, that it was directed against the State, and that its scale and effects reached the threshold of an "armed attack";[40] and (b) that it was attributable to a certain State.[41] For a State to invoke the right to take countermeasures, on the other hand, it may be sufficient to provide evidence that a cyber operation originated from a certain State and that that State did not exercise due diligence in terminating it, without necessarily having to prove attribution of the attack itself to the State.[42] In the *Nicaragua* case, the ICJ clearly explained the distinction between the objective and subjective elements from an evidentiary perspective:

> One of the Court's chief difficulties in the present case has been the determination of the facts relevant to the dispute. . . . Sometimes there is no question, in the sense that it does not appear to be disputed, that an act was done, but there are conflicting reports, or a lack of evidence, as to who did it . . . . The occurrence of the act itself may however have been shrouded in secrecy. In the latter case, the Court has had to endeavour first to establish what actually happened, before entering on the next stage of considering whether the act (if proven) was imputable to the State to which it has been attributed.[43]

The Court's observations were made against the backdrop of the secrecy that surrounded the U.S. and Nicaraguan covert operations in Central America,[44] which is also a quintessential characteristic of cyber operations.[45] In this context too, then, it is likely that evidence will be required both to establish the material elements of the wrongful act and to establish its attribution. It is still unclear, for instance, not only who is responsible for Stuxnet, but also whether the worm caused any damage and, if so, to what extent.[46] This last question is essential in order to establish whether the

---

37. *Id.* at 552.

38. 31A C.J.S. Evidence § 8 (1964).

39. *See* Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U. S.), Judgment, 1986 I.C.J. 14, para. 57 (June 27) (noting the difficulty of imputing acts to particular States).

40. *Id.* para. 195. On the distinction between "use of force" and "armed attack," see *id.* paras. 191, 195.

41. *See generally* ROSCINI, *supra* note 1, at 80–88 (discussing whether self-defense can be exercised against cyber attacks by non-state actors).

42. Geiß & Lahmann, *supra* note 34, at 635–37.

43. *Nicar. v. U.S.*, Judgment, 1986 I.C.J. para. 57.

44. *Id.*

45. *See* ROSCINI, *supra* note 1, at 38.

46. *See* Barzashka, *supra* note 21, at 48 (noting that no one has admitted to the Stuxnet attack and that the "evidence of the worm's impact . . . is circumstantial and inconclusive").

cyber operation amounted to a use of force and, more importantly, whether it was an armed attack entitling the victim State to self-defense.[47] As to establishing the subjective element of the internationally wrongful act, what is peculiar to cyber operations is that in fact three levels of evidence are needed to attribute a cyber operation to a State: First, the computer(s) or server(s) from which the operations originate must be located; second, the individual behind the operation needs to be identified; and third, it needs to be proved that the individual acted on behalf of a State so that his or her conduct is attributable to it.[48]

This leads us to an important specification: The standard of proof must be distinguished from the rules of attribution. The former is "the *quantum* of evidence necessary to substantiate the factual claims made by the parties."[49] The latter, on the other hand, determine the level of connection that must exist between an individual or group of individuals and a State for the conduct of the individuals to be attributed to the State at the international level.[50] The rules of attribution for the purposes of state responsibility have been codified in Part One of the Articles on the Responsibility of States for Internationally Wrongful Acts adopted by the International Law Commission (ILC), as well as having been articulated in the case law of the ICJ.[51] Evidence according to the applicable standard must be provided to demonstrate that the attribution test has been satisfied: In *Nicaragua*, for instance, the ICJ had to assess whether there was sufficient evidence that the United States had exercised "effective control" over the *contras* so that it could be held responsible for their violations of international humanitarian law.[52]

The standard of proof should also be distinguished from the burden of proof. The latter does not determine how much evidence, and of what type, is necessary to prove the alleged facts, but merely identifies the litigant that must provide that evidence.[53] In other words, the burden of proof is "the obligation on a party to show

---

47. See ROSCINI, *supra* note 1, at 45–63, 70–77 (describing the meaning of "use of force" and when and how a State can use self-defense).

48. *See generally id.* at 98–103.

49. James A. Green, *Fluctuating Evidentiary Standards for Self-Defence in the International Court of Justice,* 58 INT'L & COMP. L.Q. 163, 165 (2009).

50. For a discussion of the rules of attribution, see ROSCINI, *supra* note 1, at 34–40.

51. Draft Articles on Responsibilities of States for Internationally Wrongful Acts, with Commentaries, Rep. of the Int'l Law Comm'n, 53d Sess., Apr. 23–June 1, July 2–Aug. 10, 2001, pt. 1, U.N. Doc. A/56/10 (2001). For case law development, see, e.g., Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosn. & Herz. v. Serb. & Montenegro), Judgment, 2007 I.C.J. 43, paras. 392–93 (Feb. 26); Military and Paramilitary Activities in and Against Nicaragua (Nicar. V. U.S.), Judgment, 1986 I.C.J. 14, paras. 110, 393 (June 27). For further discussion, see generally ROSCINI, *supra* note 1, at 34–40.

52. *Nicar. v. U.S.*, Judgment, 1986 I.C.J. para. 115. In the *Nicaragua* case the Court did not find that there was sufficient evidence to conclude that the *contras* were totally dependent on the United States so as to qualify as de facto organs. However, it found that a situation of partial dependency,

> the exact extent of which the Court cannot establish, may certainly be inferred *inter alia* from the fact that the leaders were selected by the United States. But it may also be inferred from other factors, some of which have been examined by the Court, such as the organization, training and equipping of the force, the planning of operations, the choosing of targets and the operational support provided.

Id. para. 112.

53. ANNA RIDDELL & BRENDAN PLANT, EVIDENCE BEFORE THE INTERNATIONAL COURT OF JUSTICE 81 (2009).

that they have sufficient evidence on an issue to raise it in a case."[54] The burden of proof includes not only the "burden of persuasion,"[55] but also the "burden of production," which is the burden to produce the relevant evidence before a court.[56]

Evidence may be submitted not only to an international court or tribunal, but also to political organs (for instance, to secure a favorable vote).[57] It may also be disseminated more widely for the purposes of influencing public opinion and gaining support for certain actions or inactions.[58] One could recall the evidence presented by the Reagan Administration before the U.N. Security Council to justify its 1986 strike on Tripoli as a measure of self-defense.[59] When justifying its 2001 armed operation against Afghanistan, the U.S. Permanent Representative to the United Nations referred to the fact that the U.S. government had "clear and compelling information that the Al-Qaeda organization, which is supported by the Taliban regime in Afghanistan, had a central role in the [September 11, 2001] attacks," without, however, going into further details.[60] The same language was used by the Secretary-General of the North Atlantic Treaty Organization (NATO).[61] Evidence was also famously one of the controversial aspects of the 2003 U.S. and U.K.-led intervention in Iraq.[62] More recently, in the context of the proposed intervention to react against the use of chemical weapons in Syria, President Obama stated that "attack[ing] another country without a UN [sic] mandate and without clear evidence that can be

54. *Id.*

55. *See id.* (stating that the burden of proof is the "duty of a party to persuade").

56. Markus Benzing, *Evidentiary Issues*, *in* THE STATUTE OF THE INTERNATIONAL COURT OF JUSTICE: A COMMENTARY 1234, 1245 (Andreas Zimmermann et al., eds., 2012) [hereinafter THE STATUTE OF THE INTERNATIONAL COURT OF JUSTICE: A COMMENTARY]. As there are no parties in advisory proceedings, there is no burden of proof in this type of proceeding. Wolfrum, *supra* note 36, at 565.

57. *See* Matthew C. Waxman, *The Use of Force Against States that* Might *Have Weapons of Mass Destruction*, 31 MICH. J. INT'L L. 1, 2–3 (2009) (discussing the George W. Bush administration's unilateral approach for decisions regarding self-defense based on evidence of weapons of mass destruction (WMDs)).

58. Whether or not States have an obligation to make evidence public is a matter of debate. It has been observed that "[i]f nations are permitted to launch unilateral attacks based on secret information gained largely by inference, processed by and known only to a few individuals and not subject to international review, then Article 2(4) of the U.N. Charter is rendered virtually meaningless." Jules Lobel, *The Use of Force to Respond to Terrorist Attacks: The Bombing of Sudan and Afghanistan*, 24 YALE J. INT'L L. 537, 547 (1999). *See also* GEORGE P. FLETCHER & JENS DAVID OHLIN, DEFENDING HUMANITY: WHEN FORCE IS JUSTIFIED AND WHY 169 (2008) (noting that "[t]he principle of publicity is critical" because "there is no authority but the eyes of the world to assess" whether there was sufficient evidence to support a State's actions). *But see* Waxman, *supra* note 57, at 65 ("One practical problem frequently raised in response is that key information often cannot be disclosed publicly without compromising critical intelligence sources and methods.").

59. Lobel, *supra* note 58, at 549.

60. Permanent Rep. of the United States of America to the U.N., Letter dated 7 October 2001 from the Permanent Rep. of the United States of America to the United Nations addressed to the President of the Security Council, UN Doc S/2001/946 (Oct. 7, 2001).

61. Lord George Robertson, Statement by NATO Secretary General (Oct. 2, 2001), *available at* http://www.nato.int/docu/speech/2001/s011002a.htm.

62. *See generally* U.K. FOREIGN & COMMONWEALTH OFFICE, IRAQ'S WEAPONS OF MASS DESTRUCTION: THE ASSESSMENT OF THE BRITISH GOVERNMENT (2002) (summarizing evidence of the various weapons capabilities of the Iraqi government as of 2002); U.N. SCOR, 58th Year, 4701st mtg. at 2–17, U.N. Doc S/PV.4701 (Feb. 5, 2003) (transcribing Colin Powell's remarks to the Security Council regarding WMDs in Iraq).

presented" would raise questions of international law.[63] The political or judicial relevance of evidence may relate to the different phases of the same international dispute. For instance, the State invoking the right of self-defense against an armed attack by another State will normally try to justify the exercise of this right first before the international community and public opinion by providing evidence of the occurrence (or imminent occurrence) of the armed attack and of its attribution to the target State.[64] If, as in the *Nicaragua* case, a State subsequently brings the case before an international court which has jurisdiction over the case, the evidence will have to be assessed by that court in order to establish international responsibility and its consequences, and in particular whether the requirements for the exercise of self-defense were met.[65]

Investigations of cyber attacks among States are complicated by the absence of a uniform body of rules on the production of evidence in international law.[66] There is no treaty provision that regulates evidentiary issues in non-judicial contexts, and it is doubtful that international law has developed customary rules in that sense.[67] As to the production of evidence in inter-state litigation, non-criminal international courts normally determine their own standards in each case, which may considerably differ according to the nature of the court or the case under examination.[68] As it is not possible to identify uniform evidentiary rules applicable in all cases and before all international courts, this article will focus on proceedings before the ICJ. This is because the ICJ is the main U.N. judicial organ that deals, if the involved States have consented to its jurisdiction, with claims of state responsibility arising from the violation of any primary norm of international law.[69] The overall purpose is to establish whether rules on evidence may be identified that would apply to claims in inter-state judicial proceedings seeking remedies for damage caused by cyber

63. Julian Borger, *West Reviews Legal Options for Possible Syria Intervention Without UN Mandate,* GUARDIAN, Aug. 26, 2013, http://www.theguardian.com/world/2013/aug/26/united-nations-mandate-airstrikes-syria. Indeed, the Report of the U.N. Secretary-General's Investigation found "clear and convincing evidence" of the use of chemical weapons in the armed conflict. Rep. of the U.N. Mission to Investigate Allegations of the Use of Chemical Weapons in the Syrian Arab Republic on the Alleged Use of Chemical Weapons in the Ghouta Area of Damascus on 21 August 2013, U.N. Doc. A/67/997–S/2013/553, GAOR, 67th Sess., 8 (Sept. 16, 2013).

64. *See* Mary Ellen O'Connell, *Lawful Self-Defense to Terrorism*, 63 U. PITT. L. REV. 889, 895 (2002) [hereinafter O'Connell, *Lawful Self-Defense*] ("In many cases of self-defense, the facts of the attack and the responsible party are evident for all the world to see. Iraq's 1990 invasion of Kuwait is a case in point. When a less obvious event occurs, like the September 11 attacks, the [S]tate contemplating self-defense may have to provide evidence that future attacks are pending.").

65. *See, e.g.*, Ruth Teitelbaum, *Recent Fact-Finding Developments at the International Court of Justice*, 6 L. & PRAC. INT'L CTS. & TRIBUNALS 119, 151 (2007) (describing the International Court of Justice's (ICJ) assessment of the evidence in the *Nicaragua* case).

66. Mary Ellen O'Connell, *Evidence of Terror*, 7 J. CONFLICT & SECURITY L. 19, 21 (2002) [hereinafter O'Connell, *Evidence of Terror*].

67. *Id.*; *see also* Green, *supra* note 49, at 165 ("In general, international law does not have a clear benchmark against which the persuasiveness or reliability of evidence may be gauged for the purposes of attributing responsibility or assessing legal claims. In other words, there is no consistent standard of proof with regard to international obligations.").

68. *See* Daniel Joyce, *Fact-Finding and Evidence at the International Court of Justice: Systemic Crisis, Change or More of the Same?*, 18 FINNISH Y.B. INT'L L. 283, 286 (2007) ("The theme of flexibility dominates public international law's approach to evidence.").

69. *See, e.g.*, H. Vern Clemons, Comment, *The Ethos of the International Court of Justice is Dependent Upon the Statutory Authority Attributed to its Rhetoric: A Metadiscourse*, 20 FORDHAM INT'L L.J. 1479, 1486, 1490–91 (1997) (detailing modes of jurisdiction by the ICJ over States).

operations. It should be noted, however, that the conclusions reached with regard to the ICJ only apply to it and could not automatically be extended to other international courts.

Rules on the production of evidence before the ICJ are contained in the ICJ Statute, the Rules of Court (adopted in 1978), and Practice Directions for use by States appearing before the Court (first adopted in 2001 and subsequently amended).[70] In the following pages, the relevant rules on evidentiary issues contained in those documents, as well as those elaborated by the Court in its jurisprudence, will be applied to allegations related to cyber operations.

II. BURDEN OF PROOF AND CYBER OPERATIONS

The burden of proof identifies the litigant that has the onus of meeting the standard of proof by providing the necessary evidence.[71] Once the burden has been discharged according to the appropriate standard, the burden shifts to the other litigant, who has to prove the contrary.[72] Normally, the party that relies upon a certain fact is required to prove it (the principle *onus probandi incumbit actori*, derived from Roman law).[73] This general principle of law, invoked consistently by the ICJ and other international courts and tribunals,[74] "applies to the assertions of fact both by the Applicant and the Respondent."[75] The party bearing the burden of proof, therefore, is not necessarily the applicant (i.e., the State that has brought the application before the tribunal) but is rather the party "who . . . raised an issue,"[76] regardless of its procedural position.[77] For instance, the party (applicant or respondent) that relies on an exception, including self-defense, has the burden of proving the facts that are the basis for the exception.[78] It should also be recalled that the distinction between applicant and respondent may not always be clear in inter-

70. Rules of Court, arts. 38–89, 1978 I.C.J. Acts & Docs. 6; Statute of the International Court of Justice arts. 39–64, June 26, 1945, 33 U.N.T.S. 933; I.C.J. Practice Directions of the International Court of Justice, Practice Direction IX, 2007 Acts & Docs. 163.

71. Green, *supra* note 49, at 165.

72. *See* Roger B. Dworkin, *Easy Cases, Bad Law, and Burdens of Proof*, 25 VAND. L. REV. 1151, 1159 (1972) ("No one seems to have trouble understanding that the burden of producing evidence on one issue may shift from party to party as the case progresses.").

73. Pulp Mills on the River Uruguay (Arg. v. Uru.), Judgment, 2010 I.C.J. 14, para. 162 (Apr. 20); *see also* NATHAN D. O'MALLEY, RULES OF EVIDENCE IN INTERNATIONAL ARBITRATION: AN ANNOTATED GUIDE 203 n.34 (2012) (explaining the Roman roots of the concept).

74. Teitelbaum, *supra* note 65, at 121.

75. *Arg. v. Uru.*, 2010 I.C.J. para. 162.

76. RIDDELL & PLANT, *supra* note 53, at 89 (citing "an early indication that the Court w[ill] look carefully into which party [is] seeking to rely on certain facts, rather than relying on the traditional applicant/respondent dichotomy.").

77. According to Shabtai Rosenne, "the tendency of the Court is to separate the different issues arising in a case, treating each one separately, applying the rule *actori incumbit probatio*, requiring the party that advances a particular contention to establish it in fact and in law. The result is that each State putting forward a claim is under the general duty to establish its case, without there being any implication that such State is 'plaintiff' or 'applicant' in the sense in which internal litigation uses those terms." SHABTAI ROSENNE, THE LAW AND PRACTICE OF THE INTERNATIONAL COURT, 1920–2005, at 1200–01 (4th ed. 2006),

78. Oil Platforms (Iran v. U.S.), Judgment, 2003 I.C.J. 161, para. 57 (Nov. 6); RIDDELL & PLANT, *supra* note 53, at 87.

state litigation, especially when the case is brought before an international court by special agreement between the parties.[79]

The *onus probandi incumbit actori* principle is subject to three main limitations. First, facts that are not disputed or that are agreed upon by the parties do not need to be proven.[80] Second, the Court has relieved a party from the burden of providing evidence of facts that are "notorious" or "of public knowledge."[81] In *Nicaragua*, for instance, the Court found that "since there was no secrecy about the holding of the manoeuvres [sic], the Court considers that it may treat the matter as one of public knowledge, and as such, sufficiently established."[82] As has been noted, "the notion of common or public knowledge has, over the years, expanded, given the wide availability of information on current events in the press and on the [I]nternet."[83] Companies like McAfee, Symantec, Mandiant, and Project Grey Goose, as well as think tanks like NATO's Cooperative Cyber Defence Centre of Excellence (CCD COE), have also published reports on cyber incidents.[84] These reports essentially contain technical analysis of cyber incidents and, with the possible exception of those of the CCD COE, do not normally investigate attribution for legal purposes of those incidents in any depth (if at all).[85] The fact that cyber incidents have received extensive press coverage, as in the case of Stuxnet, may also contribute to the public knowledge character of certain facts. In *Nicaragua,* however, the ICJ warned that "[w]idespread reports of a fact may prove on closer examination to derive from a single source, and such reports, however numerous, will in such case have no greater value as evidence than the original source."[86] The ICJ has also held that the "massive body of information" available to the Court, including newspapers, radio and television reports, may be useful only when it is "wholly consistent and concordant as to the main facts and circumstances of the case."[87]

Third, the *onus probandi incumbit actori* principle only applies to facts, as opposed to the law, which does not need to be proven (*jura novit curia*).[88] It should be noted, however, that, in inter-state litigation, municipal law is a fact that must be

79. RIDDELL & PLANT, *supra* note 53, at 89.; Andrés Aguilar Mawdsley, *Evidence Before the International Court of Justice*, *in* ESSAYS IN HONOUR OF WANG TIEYA 533, 538 (Ronald St. John Macdonald ed., 1994).

80. Wolfrum, *supra* note 36, at 563.

81. *See, e.g.*, Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, para. 92 (June 27) (accepting a newspaper report as evidence of notoriety). Judicial notice has been frequently invoked by international criminal tribunals. Teitelbaum, *supra* note 65, at 144–45.

82. *Nicar. v. U.S.*, Judgment, 1986 I.C.J. para. 92.

83. RIDDELL & PLANT, *supra* note 53, at 142–43.

84. TIKK ET AL., *supra* note 14; MANDIANT, 2014 THREAT REPORT [hereinafter MANDIANT, THREAT REPORT], *available at* http://dl.mandiant.com/EE/library/WP_M-Trends2014_140409.pdf; MCAFEE, MCAFEE LABS THREATS REPORT (2014), *available at* http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q1-2014.pdf; SYMANTEC CORP., INTERNET SECURITY THREAT REPORT (2014), *available at* http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf.

85. *See generally* TIKK ET AL., *supra* note 14; MANDIANT, THREAT REPORT, *supra* note 84; MCAFEE, *supra* note 84; SYMANTEC CORP., *supra* note 84.

86. *Nicar. v. U.S.*, Judgment, 1986 I.C.J. para. 63.

87. United States Diplomatic and Consular Staff in Tehran (U.S. v. Iran), Judgment, 1980 I.C.J. 3, para. 13 (May 24).

88. Wolfrum, *supra* note 36, at 556.

proven by the parties invoking it.[89] Furthermore, the ICJ has often distinguished between treaty law and customary international law, holding that the existence and scope of customary rules—especially those of a regional character—must be proven by the parties because one of their two elements, state practice, is factual.[90] A party invoking national legislation or the existence of a general or cyber-specific custom in its favor, therefore, will bear the burden of producing relevant evidence before the Court. Certain authors have suggested that shifting the burden of proof "from the investigator and accuser to the nation in which the attack software was launched" could solve the problems of identification and attribution in the cyber context.[91] In such an approach, international law would require the State where the attack originated to prove that it neither carried out the operation nor negligently allowed others to misuse its infrastructure, as opposed to requiring the accuser to prove the contrary. Similarly, it has been argued that "[t]he fact that a harmful cyber incident is conducted via the information infrastructure subject to a nation's control is *prima facie* evidence that the nation knows of the use and is responsible for the cyber incident."[92] This, however, is not correct. First, mere knowledge does not automatically entail direct attribution, but rather merely a potential violation of the due diligence duty not to allow hostile acts from one's territory.[93] What is more, the views arguing for a reversal of the burden of proof are at odds with the *jurisprudence constante* of the ICJ.[94] In the *Corfu Channel* case, the Court famously found that the exclusive control exercised by a State over its territory "neither involves *prima facie* responsibility nor shifts the burden of proof" in relation to unlawful acts perpetrated therein.[95] The Court, however, conceded that difficulties in discharging the burden of proof in such cases may allow "a more liberal recourse to inferences of fact and circumstantial evidence."[96] This point will be further explored below in Part VI.[97] In *Armed Activities (Dem. Rep. Congo v. Uganda)*, the ICJ also did not shift the burden of proving that Zaire had been in a position to stop the armed groups' actions originating from its border regions, as claimed by Uganda in its counter-claim, from Uganda to the Democratic Republic of the Congo (DRC), and therefore found that it could not "conclude that the absence of action by Zaire's Government against the rebel groups in the border area is tantamount to 'tolerating' or 'acquiescing' in their activities."[98]

---

89. *Id.* at 557.

90. Asylum Case (Colom. v. Perú), Judgment, 1950 I.C.J. 266, 276–77 (Nov. 20); Rights of Nationals of the United States of America in Morocco (Fr. v. U.S.), Judgment 1952 I.C.J. 176, 200 (Aug. 27).

91. RICHARD A. CLARKE & ROBERT K. KNAKE, CYBER WAR: THE NEXT THREAT TO NATIONAL SECURITY AND WHAT TO DO ABOUT IT 249 (2010).

92. Daniel J. Ryan, Maeve Dion, Eneken Tikk & Julie J. C. H. Ryan, *International Cyberlaw: A Normative Approach*, 42 GEO. J. INT'L L. 1161, 1185 (2011).

93. *See* Corfu Channel (U.K. v. Alb.), Judgment, 1949 I.C.J. 4, 18 (Apr. 9) ("It cannot be concluded from the mere fact of the control exercised by a State over its territory and waters that that State necessarily knew, or ought to have known, of any unlawful act perpetrated therein . . . .").

94. *See id.* (stating that control by a State over its borders does not shift the burden of proof to the accused State).

95. *Id.*

96. *Id.*

97. *See infra* Part VI.

98. Armed Activities on the Territory of the Congo (Dem. Rep. Congo v. Uganda), Judgment, 2005 I.C.J. 168, para. 301 (Dec. 19). Judge Kooijmans wrote a separate opinion, arguing that "[i]t is for the

If one applies these findings in the cyber context, the fact that a State has exclusive "territorial" control of the cyber infrastructure from which the cyber operation originates does not per se shift the burden of proof, and it is therefore still up to the claimant to demonstrate that the territorial State is responsible for the cyber operation or that it failed to comply with its due diligence duty of vigilance, and not to the territorial State to demonstrate the contrary.[99]

Even beyond the principle of territorial control, the fact that relevant evidence is in the hands of the other party does not per se shift the burden of proof. In the *Avena* case, the ICJ held that it could not

> accept that, because such information may have been in part in the hands of Mexico, it was for Mexico to produce such information. It was for the United States to seek such information, with sufficient specificity, and to demonstrate both that this was done and that the Mexican authorities declined or failed to respond to such specific requests.... The Court accordingly concludes that the United States has not met its burden of proof in its attempt to show that persons of Mexican nationality were also United States nationals.[100]

The fact that cyber operations were conducted in the context of an armed conflict, as was the case of those against Georgia in 2008,[101] also does not affect the normal application of the burden of proof.[102] In *Nicaragua*, the ICJ recalled the *Corfu Channel* and *Tehran Hostages* judgments and found that "[a] situation of armed conflict is not the only one in which evidence of fact may be difficult to come by, and the Court has in the past recognized and made allowance for this...."[103] Even in such circumstances, therefore, "it is the litigant seeking to establish a fact

---

State under a duty of vigilance to show what efforts it has made to fulfill that duty and what difficulties it has met" and concluding that the Democratic Republic of the Congo (DRC) had not provided evidence to show that it had adopted "credible measures" to prevent transborder attacks. Armed Activities on the Territory of the Congo (Dem. Rep. Congo v. Uganda), Judgment, 2005 I.C.J. 306, paras. 82–83 (Dec. 19) (separate opinion of Judge Kooijmans).

99. It should not be forgotten that cyberspace consists of a physical and a syntactic (or logical) layer: The former includes the physical infrastructure through which the data travel wired or wireless, including servers, routers, satellites, cables, wires, and the computers, while the latter includes the protocols that allow data to be routed and understood, as well as the software used and the data. David J. Betz & Tim Stevens, *Analogical Reasoning and Cyber Security*, 44 SECURITY DIALOGUE 147, 151 (2013). Cyber operations can then be seen as "the reduction of information to electronic format and the actual movement of that information between physical elements of cyber infrastructure." NILS MELZER, UNIDIR RES., CYBERWARFARE AND INTERNATIONAL LAW 5 (2011), *available at* http://www.isn.ethz.ch/Digital-Library/Publications/ Detail/?lng=en&id=134218. In its 2013 Report, the Group of Governmental Experts established by the UN General Assembly confirmed that "State sovereignty and international norms and principles that flow from sovereignty apply to State conduct of ICT-related activities, and to their jurisdiction over ICT infrastructure within their territory." Rep. of the Group of Gov. Experts on Devs. in the Field of Info. and Telecomm. in the Context of Int'l Sec., 68th Sess., 8, U.N. Doc. A/68/98 (June 24, 2013).

100. Avena and Other Mexican Nationals (Mex. v. U.S.), Judgment, 2004 I.C.J. 12, para. 57 (Mar. 31).

101. Markoff, *supra* note 13.

102. *See generally* Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14 (June 27).

103. Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1984 I.C.J. 392, para. 101 (Nov. 26).

who bears the burden of proving it . . . ."[104] In the *El Salvador/Honduras* case, the Court stated that it

> fully appreciates the difficulties experienced by El Salvador in collecting its evidence, caused by the interference with governmental action resulting from acts of violence. It cannot however apply a presumption that evidence which is unavailable would, if produced, have supported a particular party's case; still less a presumption of the existence of evidence which has not been produced.[105]

The application of the *onus probandi incumbit actori* principle is also not affected by the possible asymmetry in the position of the litigants in discharging the burden of proof due to the fact that one has acted covertly (as is virtually always the case of cyber operations).[106] As Judge Owada points out in his Separate Opinion attached to the *Oil Platforms* judgment, however, the Court should "take a more proactive stance on the issue of evidence and that of fact-finding" in such cases in order to ensure that the rules of evidence are applied in a "fair and equitable manner" to both parties.[107]

Finally, it has been argued that a reversal of the burden of proof may derive from an application of the precautionary principle based on international environmental law in cyberspace.[108] The precautionary principle entails "the duty to undertake all appropriate regulatory and other measures at an early stage, and well before the (concrete) risk of harm occurs."[109] On this view, States would have an obligation to implement measures to prevent the possible misuse of their cyber infrastructure, in particular by establishing a national cyber security framework.[110] Regardless of whether the precautionary principle, with its uncertain normativity, extends to cyberspace,[111] it still would not lead to a reversal of the burden of proof from the claimant to the State from which a cyber operation originates. In the *Pulp Mills* case, the ICJ concluded that "while a precautionary approach may be relevant in the interpretation and application of the provisions of the Statute [of the River Uruguay], it does not follow that it operates as a reversal of the burden of proof."[112]

---

104. *Id.*

105. Land, Island and Maritime Frontier Dispute (El Sal./Hond.: Nicar. intervening), Judgment, 1992 I.C.J. 351, para. 63 (Sept. 11).

106. Oil Platforms (Iran v. U.S.), Judgment, 2003 I.C.J. 306, para. 46 (Nov. 6); (separate opinion of Judge Owada).

107. *Id.* para. 47.

108. *See* Thilo Marauhn, *Customary Rules of International Environmental Law – Can They Provide Guidance for Developing a Peacetime Regime for Cyberspace?*, *in* PEACETIME REGIME FOR STATE ACTIVITIES IN CYBERSPACE, *supra* note 34, at 475 (describing the precautionary approach's relationship to international environmental law).

109. Katharina Ziolkowski, *General Principles of International Law as Applicable in Cyberspace*, *in* PEACETIME REGIME FOR STATE ACTIVITIES IN CYBERSPACE, *supra* note 34, at 169.

110. *Id.*

111. *See* Marauhn, *supra* note 108, at 475–76 (asserting doubt that the precautionary principle applies to cyberspace).

112. Pulp Mills on the River Uruguay (Arg. v. Uru.), Judgment, 2010 I.C.J. 14, para. 164 (Apr. 20).

The Court, however, did not specify whether the precautionary principle might result in at least a lowering of the standard of proof.[113]

In light of the above discussion, it can be concluded that it is unlikely that the ICJ would accept that there is a reversal of the burden of proof in the cyber context. As has been correctly argued, "suggesting a reversal of the burden of proof could easily lead to wrong and even absurd results given the possibility of routing cyber operations through numerous countries, and to the denouncing of wholly uninvolved and innocent States."[114] In the case of the 2007 DDoS campaign against Estonia, for instance, the botnets included computers located not only in Russia, but also in the United States, Europe, Canada, Brazil, Vietnam and other countries.[115] Difficulties in discharging the burden of proof, which are particularly significant in the context under examination, may, however, result in an alleviation of the standard of proof required to demonstrate a particular fact. It is to this aspect that the analysis now turns.

III. STANDARD OF PROOF AND CYBER OPERATIONS

It is well known that, while in civil law systems there are no specific standards of proof that judges have to apply because they are authorized to evaluate the evidence produced according to their personal convictions on a case-by-case basis, common law jurisdictions employ a rigid classification of standards.[116] From the most to the least stringent, these include: beyond reasonable doubt (i.e., indisputable evidence, a standard used in criminal trials), clear and convincing (or compelling) evidence (i.e., more than probable but short of indisputable), and the preponderance of evidence or balance of probabilities (i.e., more likely than not or reasonably probable, a standard normally used in civil proceedings).[117] A fourth standard is that of *prima facie* evidence—a standard that merely requires indicative proof of the correctness of the contention made.[118]

The Statute of the ICJ and the Rules of Court neither require specific standards of proof nor indicate what methods of proof the Court will consider as being probative in order to meet a certain standard.[119] The ICJ has to date avoided clearly indicating the standards of proof expected from the litigants during the proceedings.[120] It has normally referred to the applicable standard of proof in the

113. *See id.* (discussing the applicability of the precautionary principle to the burden of proof).

114. Geiß & Lahmann, *supra* note 34, at 628.

115. U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES, *supra* note 8, at 173.

116. Marko Milanović, *State Responsibility for Genocide*, 17 EUR. J. INT'L L. 553, 594 (2006).

117. Mary Ellen O'Connell, *Rules of Evidence for the Use of Force in International Law's New Era*, 100 AM. SOC'Y INT'L L. PROC. 44, 45 (2006) [hereinafter O'Connell, *Rules of Evidence*]; Milanović, *supra* note 116, at 594; Green, *supra* note 49, at 167.

118. Green, *supra* note 49, at 166; Geiß & Lahmann, *supra* note 34, at 624.

119. *See generally* Statute of the International Court of Justice, June 26, 1945, 33 U.N.T.S. 933; Rules of Court, 1978 I.C.J. Acts & Docs. 6.

120. That approach has been criticized by judges from common law countries. *See, e.g.*, Oil Platforms (Iran v. U.S.), 2003 I.C.J. 270, paras. 42–44 (Nov. 6) (separate opinion of Judge Buergenthal) (stating that the Court failed to explain a standard of proof); Oil Platforms (Iran v. U.S.), 2003 I.C.J. 225, paras. 30–39 (Nov. 6)(separate opinion of Judge Higgins) (criticizing the court for not stating a standard of proof).

judgments, but at that point it is of course too late for the parties to take it into account in pleading their cases.[121]

There is no agreement on what standard of proof the ICJ should expect from the parties in the cases before it.[122] If, because of their nature, international criminal courts use the beyond reasonable doubt standard in their proceedings,[123] the most appropriate analogy for inter-state litigation is not with criminal trials, but with certain types of civil litigation.[124] In his Dissenting Opinion in the *Corfu Channel* case, Judge Krylov suggested that "[o]ne cannot condemn a State on the basis of probabilities. To establish international responsibility, one must have clear and indisputable facts."[125] Wolfrum has argued that, while the jurisdiction of an international court over a case should be established beyond reasonable doubt, the ICJ has generally applied a standard comparable to that of preponderance of evidence used in domestic civil proceedings when deciding disputes involving state responsibility.[126] Others have maintained that such a standard only applies to cases not concerning attribution of international wrongful acts, such as border delimitations, and that when international responsibility is at stake, the standard is stricter and requires clear and convincing evidence.[127]

It is therefore difficult, and perhaps undesirable,[128] to identify a uniform standard of proof generally applicable in inter-state litigation or even a predominant one: the Court "tends to look at issues as they arise."[129] This case-by-case approach, however, does not exclude that a standard of proof may be identified having regard to the primary rules in dispute, i.e., "the substantive rules of international law through . . . which the Court will reach its decision."[130] Indeed, when the allegation is the same, it seems logical that the evidentiary standard should also be the same.[131] There are indications, for instance, that claims related to *jus ad bellum* violations, in particular in relation to the invocation of an exception to the prohibition of the use of

121. *See* Teitelbaum, *supra* note 65, at 124 ("The Court's determination of the standard of proof may be said to be made on an *ad hoc* basis, and is only revealed at the end of the process when the Court delivers its judgment."). It has been suggested that "the Court might consider whether, either prior to the submission of written pleadings, after the first round of written pleadings, or prior to the oral hearings, it should ask the parties to meet a specific burden of proof for certain claims." *Id.* at 128).

122. H.E. Judge Rosalyn Higgins, President, Int'l Court of Justice, Speech to the Sixth Committee of the General Assembly 4 (Nov. 2, 2007).

123. Wolfrum, *supra* note 36, at 569.

124. Waxman, *supra* note 57, at 59.

125. Corfu Channel (U.K. v. Alb.), Judgment, 1949 I.C.J. 4, 72 (Apr. 9) (dissenting opinion of Judge Krylov).

126. Wolfrum, *supra* note 36, at 566.

127. RIDDELL & PLANT, *supra* note 53, at 133.

128. Green, *supra* note 49, at 167.

129. Sir Arthur Watts, *Burden of Proof, and Evidence before the ECJ*, *in* IMPROVING WTO DISPUTE SETTLEMENT PROCEDURES: ISSUES AND LESSONS FROM THE PRACTICE OF OTHER INTERNATIONAL COURTS AND TRIBUNALS 289, 294 (Friedl Weiss ed., 2000).

130. ROSENNE, *supra* note 77, at 1043. In Ahmadou Sadio Diallo (Guinea v. Dem. Rep. Congo), Judgment, 2010 I.C.J. 639, para. 54 (Nov. 30), the ICJ makes a similar point with regard to the burden of proof.

131. *See* Green, *supra* note 49, at 169–71 (suggesting that one consistent standard should apply to all cases of self-defense—whatever magnitude the consequences of the violation of the prohibition of the use of force might have—both to the objective and subjective elements of the internationally wrongful act).

force in international relations, have been treated as requiring "'clear and convincing evidence."[132] In the *Nicaragua* judgment, the Court referred to "convincing evidence" of the facts on which a claim is based and to the lack of "clear evidence" of the degree of control exercised by the United States over the *contras*.[133] In the *Oil Platforms* case, the ICJ rejected evidence with regard to Iran's responsibility for mine laying that was "highly suggestive, but not conclusive," holding that "evidence indicative of Iranian responsibility for the attack on the *Sea Isle City*" was insufficient.[134] In *Dem. Rep. Congo v. Uganda*, the ICJ referred again to facts "convincingly established by the evidence," "convincing evidence," and "evidence weighty and convincing."[135] Beyond the ICJ, the Eritrea-Ethiopia Claims Commission also found that there was "clear" evidence that events in the vicinity of Badme were minor incidents and did not reach the magnitude of an armed attack.[136] The above suggests that at least clear and convincing evidence is expected for claims related to the use of force. As self-defense is an exception to the prohibition of the use of force, in particular, the standard of proof should be high enough to limit its invocation to exceptional circumstances and thus avoid abuses.[137]

If clear and convincing evidence is required at least for claims related to the use of armed force, the question arises whether there is a special, and lower, standard in the cyber context, in particular for claims of self-defense against cyber operations. Indeed, "evidentiary thresholds that might have worked well in a world of conventional threats—where capabilities could be judged with high accuracy and the costs of false negatives to peace and security were not necessarily devastating—risk exposing States to unacceptable dangers."[138] There is of course no case law in relation to claims arising out of inter-state cyber operations,[139] so possible indications in this sense have to be found elsewhere. The Project Grey Goose Report on the 2008 cyber operations against Georgia, for instance, relies on the concordance of various pieces of circumstantial evidence to suggest that the Russian government was

132. O'Connell, *Evidence of Terror*, *supra* note 66, at 22; *see also* Teitelbaum, *supra* note 65, at 125–26 (discussing an ICJ case in which the Court applied a standard "similar to" clear and convincing).

133. Green, *supra* note 49, at 172; *see also* Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, paras. 24, 29, 62, 109 (June 27) (mentioning both "convincing" and lack of "clear" evidence).

134. Oil Platforms (Iran v. U.S.), Judgment, 2003 I.C.J. 161, paras. 71, 61 (Nov. 6). *See also* Green, *supra* note 49, at 172–73; Teitelbaum, *supra* note 65, at 125–26 (arguing that the ICJ uses a clear and convincing standard of evidence).

135. Armed Activities on the Territory of the Congo (Dem. Rep. Congo v. Uganda), Judgment, 2005 I.C.J. 168, paras. 72, 91, 136 (Dec. 19). Confusingly, however, in other parts of the Judgment the Court seemed to employ a *prima facie* or preponderance of evidence standard, in particular when it had to determine whether the conduct of armed groups against the DRC was attributable to Uganda. Green, *supra* note 49, at 175–76.

136. Partial Award—Jus Ad Bellum: Ethiopia's Claims 1–8 (Eth. v. Eri.), 26 R.I.A.A. 459, para. 12 (Eri. Eth. Cl. Comm. 2005); *See* O'Connell, *Rules of Evidence*, *supra* note 117117, at 45 (discussing the evidence standard decided in the Ethiopia-Eritrea Jus Ad Bellum Claim).

137. O'Connell, *Lawful Self-Defense*, *supra* note 64, at 898.

138. Waxman, *supra* note 57, at 62. The author argues that "the required degree of certainty about capability ought to vary with certainty about intent." *Id.* at 61. Transposed in the cyber context, when the likelihood that an adversary will be able and willing to use cyber weapons is higher, less evidence will be required to prove it.

139. Herbert Lin, *Cyber Conflict and International Humanitarian Law*, 94 INT'L REV. RED CROSS 515, 524 (2012).

responsible for the operations.[140] In its reply to the U.N. Secretary-General on issues related to information security, the United States claimed that "high-confidence attribution of identity to perpetrators cannot be achieved in a timely manner, if ever, and success often depends on a high degree of transnational cooperation."[141] In a Senate questionnaire fulfilled in preparation for a hearing on his nomination to head of the U.S. Cyber Command, Lieutenant General Keith Alexander argued that "some level of mitigating action" can be taken against cyber attacks "even when we are not certain who is responsible."[142] Similar words were employed by his successor, Vice Admiral Michael S. Rogers: "International law does not require that a nation know who is responsible for conducting an armed attack before using capabilities to defend themselves from that attack."[143] However, Vice Admiral Rogers also cautioned that, "from both an operational and policy perspective, it is difficult to develop an effective response without a degree of confidence in attribution."[144] Overall, the above views seem to suggest an evidentiary standard, based on circumstantial evidence, significantly lower than clear and convincing evidence and even lower than a preponderance of the evidence, on the basis that identification and attribution are more problematic in a digital environment than in the analog world.[145]

It is difficult, however, to see why the standard of proof should be lower simply because it is more difficult to reach it. The standard of proof exists not to disadvantage the claimant, but to protect the respondent against false attribution, which, thanks to tricks like IP spoofing,[146] onion routing,[147] and the use of botnets,[148] is a particularly serious risk in the cyber context. The views mentioned above are also far from being unanimously held, even within the U.S. government: The Air Force

---

140. *See generally* PROJECT GREY GOOSE, RUSSIA/GEORGIA CYBER WAR—FINDINGS AND ANALYSIS (PHASE I REPORT) (2008), *available at* http://www.scribd.com/doc/6967393/Project-Grey-Goose-Phase-I-Report.

141. *Developments in the Field of Information and Telecommunications*, *supra* note 3, at 17.

142. Advance questions for Lieutenant General Keith Alexander for Commander, USA Nominee for Commander, U.S. Cyber Command, S. Comm. Armed Servs. 12 (Apr. 15, 2010), https://epic.org/privacy/nsa/Alexander_04-15-10.pdf.

143. Advance Questions for Vice Admiral Michael S. Rogers, USN Nominee for Commander, U.S. Cyber Command, S. Comm. Armed Servs. (Mar. 11, 2014), http://www.armed-services.senate.gov/imo/media/doc/Rogers_03-11-14.pdf.

144. *Id.*

145. *See, e.g.*, David E. Graham, *Cyber Threats and the Law of War*, 4 J. NAT'L SECURITY L. & POL'Y 87, 93 (2010) ("Given the difficulties raised by the traditional requirement to attribute cyber attacks conclusively and directly to a state . . . there is now a growing effort to formulate acceptable alternatives to the notion of 'conclusive attribution.'"). The author seems, however, to confuse attribution criteria and standards of evidence.

146. *See* Bradley Raboin, *Corresponding Evolution: International Law and the Emergence of Cyber Warfare*, 31 J. NAT'L ASS'N ADMIN. L. JUDICIARY 602, 614–15 (2011) ("IP spoofing is a kind of hijacking technique that allows the hacking user to operate a computer while appearing as a trusted host. By thus concealing his true identity, the hacker can gain access to computer networks and network resources.").

147. *See* Christopher Riley, *The Need for Software Innovation Policy*, 5 J. TELECOMM. & HIGH TECH. L. 589, 607 (2007) ("Onion routing protects the anonymity of an Internet user by routing messages through multiple intermediate nodes. Each intermediate node hides the origin of messages in such a way that a reply message can reach the original source node, and yet no node knows more of the path of the message than the nodes immediately before and after it on the message path.").

148. *See* Derek E. Bambauer, *Ghost in the Network*, 162 U. PA. L. REV. 1011, 1034 n.158 (2014) ("A botnet is a set of computers that have been infected with malware and that are controlled by someone other than their users.").

Doctrine for Cyberspace Operations, for instance, States that attribution of cyber operations should be established with "sufficient confidence and verifiability."[149] A report prepared by Italy's Parliamentary Committee on the Security of the Republic goes further and requires it to be demonstrated "*in modo inequivocabile*" (unequivocally) that an armed attack by cyber means originated from a State and was undertaken on the instruction of governmental bodies.[150] The document also suggests that attribution to a State requires "*«prove» informatiche inconfutabili*" ("irrefutable digital «evidence»"), which, the Report concedes, is a standard that is very difficult to meet.[151] Germany also highlighted the danger of a lack of "reliable attribution" of malicious cyber activities in creating opportunities for "false flag attacks," misunderstandings, and miscalculations.[152] In relation to the DDoS attacks against Estonia, a U.K. House of Lords document lamented that "the analysis of today is really very elusive, not *conclusive* and it would still be very difficult to act on it."[153] Finally, the AIV/CAVV Report, which has been endorsed by the Dutch government,[154] requires "reliable intelligence . . . before a military response can be made to a cyber attack" and "sufficient certainty regarding the identity of the author of the attack."[155] In its response to the Report, the Dutch government argued that self-defense can be exercised against cyber attacks "only if the origin of the attack and the identity of those responsible are sufficiently certain."[156]

All in all, clear and convincing evidence seems the appropriate standard not only for claims of self-defense against traditional armed attacks, but also for those against cyber operations: a *prima facie* or preponderance of evidence standard might lead to specious claims and false or erroneous attribution, while a beyond reasonable doubt standard would be unrealistic. In the *Norwegian Loans* case, Judge Lauterpacht emphasized that "the degree of burden of proof . . . adduced ought not to be so stringent as to render the proof unduly exacting."[157] As explained by

149. U.S. AIR FORCE, CYBERSPACE OPERATIONS: AIR FORCE DOCTRINE DOCUMENT 3-12, at 10 (2010).

150. COMITATO PARLAMENTARE PER LA SICUREZZA DELLA REPUBBLICA, RELAZIONE SULLE POSSIBILI IMPLICAZIONI E MINACCE PER LA SICUREZZA NAZIONALE DERIVANTI DALL'UTILIZZO DELLO SPAZIO CIBERNETICO 26 (2010), *available at* http://www.parlamento.it/documenti/repository/commissioni/bicamerali/COMITATO%20SICUREZZA/Doc_XXXIV_n_4.pdf.

151. *Id.*

152. Letter from the Permanent Mission of the Fed. Republic of Ger. to the United Nations addressed to the Office for Disarmament Affairs, Note No. 516/2012 (Nov. 5, 2012). Laurie R. Blank, *International Law and Cyber Threats from Non-State Actors*, 89 INT'L L. STUD. 406, 417 (2013) ("[T]he victim State must tread carefully and seek as much clarity regarding the source of the attack as possible to avoid launching a self-defense response in the wrong direction.").

153. EUROPEAN UNION COMMITTEE, PROTECTING EUROPE AGAINST LARGE-SCALE CYBER-ATTACKS, 2009–2010, H.L. 68, at 42 (emphasis added).

154. Michael N. Schmitt, *The Law of Cyber Warfare:* Quo Vadis*?*, 25 STAN. L. & POL'Y REV. 269, 280 n.40 (2014); *Government Response to the AIP/CAVV Report on Cyber Warfare*, RIJKSOVERHEID (Apr. 26, 2012), http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/rapporten/2012/04/26/cavv-advies-nr-22-bijlageregeringsreactie-en/cavv-advies-22-bijlage-regeringsreactie-en.pdf (Netherlands) [hereinafter GOV'T OF THE NETH.].

155. ADVISORY COUNCIL ON INT'L AFFAIRS & ADVISORY COMM. ON ISSUES OF PUB. INT'L LAW, CYBER WARFARE 22 (2011).

156. GOV'T OF THE NETH., *supra* note 154, at 5. The CCD COE Report on Georgia also concludes that "there is no *conclusive* proof of who is behind the DDoS attacks, even though finger pointing at Russia is prevalent by the media." TIKK ET AL., *supra* note 14, at 12 (emphasis added).

157. Certain Norwegian Loans (Fr. v. Nor.), Judgment, 1957 I.C.J. 9, 39 (July 6) (separate opinion of

Michael Schmitt, a clear and convincing standard "obliges a state to act reasonably, that is, in a fashion consistent with the normal state practice in same or similar circumstances. Reasonable States neither respond precipitously on the basis of sketchy indications of who has attacked them nor sit back passively until they have gathered unassailable evidence."[158]

Those who criticize a clear and convincing evidence standard for the exercise of self-defense against cyber operations would rely on the fact that, due to the speed at which such operations may occur and produce their consequences, the requirement of a high level of evidence may in fact render it impossible for the victim State safely to exercise its right of self-defense. Such concerns, however, are exaggerated. Indeed, if the cyber attack was a standalone event that instantaneously produced its damaging effects, a reaction in self-defense would not be necessary. If, on the other hand, the cyber attack were continuing or formed of a series of smaller scale cyber attacks,[159] the likelihood that clear and convincing evidence could be collected would considerably increase.[160]

However, there are also indications that the most serious allegations, such as those involving international crimes, require a higher standard to discharge the burden of proof.[161] As Judge Higgins wrote in her separate opinion attached to the *Oil Platforms* Judgment, "the graver the charge the more confidence must there be in the evidence relied on . . . ."[162] In *Corfu Channel*, the Court appeared to suggest that the standard of proof is higher for charges of "exceptional gravity against a State."[163] In the *Bosnian Genocide* case, the ICJ confirmed that "claims against a State involving charges of exceptional gravity must be proved by evidence that is *fully conclusive* . . . . The same standard applies to the proof of attribution for such acts" (and accordingly applies both to the objective and subjective elements of an international crime) (emphasis added).[164] The Court also found that assistance

Judge Sir Hersch Lauterpacht).

158. Schmitt's exact verbiage calls for a "clear and compelling" standard. Michael N. Schmitt, *Cyber Operations and the* Jus Ad Bellum *Revisited*, 56 VILL. L. REV 569, 595 (2011).

159. On the application of the doctrine of accumulation of events to cyber operations, see ROSCINI, *supra* note 1, at 108–10.

160. *See* Yoram Dinstein, Professor Emeritus, Tel Aviv University, Cyber War and International Law, Concluding Remarks at the 2012 Naval War College International Law Conference, *in* 89 INT'L L. STUD. 276, 282 (2013) (exemplifying similar reasoning in relation to the identification of the State responsible for the cyber attack).

161. *Contra* Prisoners of War–Eritrea's Claim 17 (Eth. v. Eri.), Partial Award, 26 R.I.A.A. 23, paras. 45–47 (Eri. Eth. Cl. Comm. 2003) (deciding to require clear and convincing evidence, as opposed to a higher burden of proof, because the Commission is "not a criminal tribunal").

162. Oil Platforms (Iran v. U.S.), Judgment, 2003 I.C.J. 225, para. 33 (Nov. 6) (separate opinion of Judge Higgins).

163. Corfu Channel (U.K. v. Alb.), Judgment, 1949 I.C.J. 4, 17 (Apr. 9). This interpretation of the Court's judgment, however, is not uncontroversial. *See* Andrea Gattini, *Evidentiary Issues in the ICJ's* Genocide *Judgment*, 5 J. INT'L CRIM. JUST. 889, 896 (2007) ("The Court somehow hid behind a quotation from the *Corfu Channel* case, where it had been stated that 'a charge of such exceptional gravity against a State would require a degree of certainty that has not been reached here.'").

164. Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosn. & Herz. v. Serb. & Montenegro), Judgment, 2007 I.C.J. 43, para. 209 (Feb. 26) (emphasis added); *see also U.K. v. Alb.*, 1949 I.C.J. at 17. It is not entirely clear whether the Court linked the notion of gravity to the importance of the norm allegedly breached or the magnitude of the violation. It would seem more correct to refer to the gravity as linked to the former, as, if the evidentiary standard depended on the

provided by Yugoslavia to the Bosnian Serbs had not been "established beyond any doubt."[165] Gravity is, of course, inherent in any *jus cogens* violation.[166] Claims of reparation for cyber operations qualifying as war crimes, crimes against humanity, or acts of genocide, therefore, should require fully conclusive evidence, not just evidence that is clear and convincing. As has been aptly suggested, however, "[a] higher standard of proof may only be justified if the Court is willing to balance this strict approach with a more active use of its fact-finding powers to make sure that claims for breaches of *jus cogens* norms are not doomed to fail merely on evidential grounds."[167]

In the *Bosnian Genocide* judgment, the Court also appeared to make a distinction between a violation of the prohibition of committing acts of genocide, for which evidence must be "fully conclusive," and a violation of the obligation to prevent acts of genocide, where the Court required "proof at a high level of certainty appropriate to the seriousness of the allegation,"[168] even though not necessarily fully conclusive evidence.[169] Such an approach appears justified by the different nature of the obligation breached: Indeed, presumptions and inferences necessarily play a more significant role when the wrongful act to be proved consists of an omission, as is the case of the breach of an obligation to prevent.[170] By the same token, it may be suggested that the standard of proof required to prove that a State has conducted cyber operations amounting to international crimes is higher than that required to prove that it did not exercise the necessary due diligence to stop its cyber infrastructure from being used by others to commit international crimes.

IV. METHODS OF PROOF AND CYBER OPERATIONS

What type of evidence may be relied on in order to meet the required standard of proof and establish that a cyber operation has occurred, has produced damage, and is attributable to a certain State or non-state actor? The production of evidence before the ICJ is regulated by Articles 48 to 52 of its Statute and by the Rules of Court. There is, however, no list of the methods of proof available to parties before the Court nor any indication of their different probative weight.[171] Article 48 of the ICJ Statute provides only that "[t]he Court shall . . . make all arrangements

---

latter, "some States could have a perverse incentive to sponsor more devastating attacks so as to raise the necessary burden of proof and potentially defeat accountability." Shackelford & Andres, *supra* note 34, at 990.

165. *Bosn. & Herz. v. Serb. & Montenegro*, 2007 I.C.J. para. 422.

166. *See* Sévrine Knuchel, *State Immunity and the Promise of* Jus Cogens, 9 NW. J. INT'L HUM. RTS. 149, 172 (2011) (describing the *Ferrini* case, which illustrates the Court's "reli[ance] on *jus cogens* not as a conflict rule, but rather as a means of highlighting the seriousness of the acts committed by the foreign State . . . .").

167. Benzing, *supra* note 56, at 1266.

168. *Bosn. & Herz. v. Serb. & Montenegro*, 2007 I.C.J. paras. 209–10.

169. Benzing, *supra* note 56, at 1266.

170. Gattini, *supra* note 163, at 899. In *Nicaragua*, the Court had already found that the fact that Nicaragua had to prove a negative (the non-supply of arms to rebels in neighboring countries) had to be borne in mind when assessing the evidence. Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U. S.), Judgment, 1986 I.C.J. 14, para. 147 (June 27).

171. *Compare* Statute of the International Court of Justice arts. 48–52, June 26, 1945, 33 U.N.T.S. 933, *and* Rules of Court, arts. 57, 58, 62–64, 71, 1978 I.C.J. Acts & Docs. 6 (together demonstrating that there are no methods of proof for dealing with the production of evidence before the ICJ).

connected with the taking of evidence,"[172] while Article 58 of the Rules of Court confirms that "the method of handling the evidence and of examining any witnesses and experts . . . shall be settled by the Court after the views of the parties have been ascertained in accordance with Article 31 of these Rules."[173]

As a leading commentator has observed, "[t]he International Court of Justice has construed the absence of restrictive rules in its Statute to mean that a party may generally produce any evidence as a matter of right, so long as it is produced within the time limits fixed by the Court."[174] Although it is primarily the parties' responsibility to produce the evidence necessary to prove the facts alleged, the Court may also order the production of documents, call experts and witnesses, conduct site visits, and request relevant information from international organizations.[175] In *Nicaragua*, for instance, the Court found that it was "not bound to confine its consideration to the material formally submitted to it by the parties."[176] In that judgment, the ICJ also emphasized the principle of free assessment of evidence, stating that "within the limits of its Statute and Rules, [the Court] has freedom in estimating the value of the various elements of evidence . . . ."[177]

In the next pages, methods of proof that may be relevant in relation to cyber operations will be examined.

A. Documentary Evidence

Although there is no formal hierarchy between different sources, the ICJ has taken a civil law court approach and has normally given primacy to written documents over oral evidence.[178] Documentary evidence includes "all information submitted by the parties in support of the contentions contained in the pleadings other than expert and witness testimony."[179] According to Shabtai Rosenne, documentary evidence can be classified in four categories:

> published treaties included in one of the recognized international or national collections of treaty texts; official records of international organizations and of national parliaments; published and unpublished diplomatic correspondence, and communiqués and other miscellaneous materials, including books, maps, plans, charts, accounts, archival material,

172. Statute of the International Court of Justice art. 48, June 26, 1945, 33 U.N.T.S. 933.

173. Rules of the Court, art. 58, 2007 I.C.J. Acts & Docs. 91.

174. DURWARD V. SANDIFER, EVIDENCE BEFORE INTERNATIONAL TRIBUNALS 184 (rev. ed. 1975).

175. Statute of the International Court of Justice arts. 49, 50, June 26, 1945, 33 U.N.T.S. 933; Rules of Court, arts. 62, 66, 67, 69, 1978 I.C.J. Acts & Docs. 6.

176. Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, para. 30 (June 27). *See* Statute of the International Court of Justice art. 49, June 26, 1945, 33 U.N.T.S. 933; Rules of the Court, art. 62, 2007 I.C.J. Acts & Docs. 91.

177. *Nicar. v. U.S.*, 1986 I.C.J. para. 60. *See also* Armed Activities on the Territory of the Congo (Dem. Rep. Congo v. Uganda), Judgment, 2005 I.C.J. 168, para. 59 (Dec. 19) (explaining the Court's own considerations regarding the weight of the evidence).

178. RIDDELL & PLANT, *supra* note 53, at 232; Aguilar Mawdsley, *supra* note 79, at 543.

179. Wolfrum, *supra* note 36, at 558.

> photographs, films, legal opinions and opinions of experts, etc.; and affidavits and declarations.[180]

Although the Court has the power to call upon the parties to produce any evidence it deems necessary or to seek such evidence itself, it has normally refrained from doing so and has relied on that spontaneously produced by the litigants.[181] All documents not "readily available" must be produced by the interested party.[182] A "publication readily available" is a document "available in the public domain . . . in any format (printed or electronic), form (physical or on-line, such as posted on the internet) or on any data medium (on paper, on digital or any other media) . . . [that] should be accessible in either of the official languages of the Court," and which it is possible to consult "within a reasonably short period of time."[183] The accessibility should be assessed in relation to the Court and the other litigant.[184] The fact that a publication is "readily available" does not necessarily render the concerned facts public knowledge, but rather relieves the party from the burden of having to produce it.[185] The facts, however, still need to be proved.[186]

Official state documents, such as national legislation, cyber doctrines, manuals, strategies, directives and rules of engagement, may become relevant in establishing state responsibility for cyber operations.[187] In *Nicaragua*, for instance, the responsibility of the United States for encouraging violations of international humanitarian law was established on the basis of the publication of a manual on psychological operations.[188] According to the Court, "[t]he publication and dissemination of a manual in fact containing the advice quoted above must . . . be regarded as an encouragement, which was likely to be effective, to commit acts

---

180. ROSENNE, *supra* note 77, at 1246 (footnotes omitted). In the *Bosnian Genocide* Judgment, the Court noted that the parties had produced

> reports, resolutions and findings by various United Nations organs, including the Secretary-General, the General Assembly, the Security Council and its Commission of Experts, and the Commission on Human Rights, the Sub-Commission on the Prevention of Discrimination and Protection of Minorities and the Special Rapporteur on Human Rights in the former Yugoslavia; documents from other inter-governmental organizations such as the Conference for Security and Co-operation in Europe; documents, evidence and decisions from the ICTY; publications from governments; documents from non-governmental organizations; media reports, articles and books.

Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosn. & Herz. v. Serb. & Montenegro), Judgment, 2007 I.C.J. 43, para. 211 (Feb. 26); *see also Dem. Rep. Congo v. Uganda*, 2005 I.C.J. para. 60.

181. Practice Directions of the International Court of Justice, Practice Direction IX bis, paras. (2)(i)–(ii), 2007 Acts & Docs. 163.

182. *Id.*

183. *Id.*

184. *Id.*

185. Rules of Court, art. 56(4), 1978 I.C.J. Acts & Docs. 6. Benzing, *supra* note 56, at 1241.

186. Benzing, *supra* note 56, at 1241.

187. *See* Mark D. Young, *National Cyber Doctrine: The Missing Link in the Application of American Cyber Power*, J. NAT'L SECURITY L. & POL'Y 173, 175–76 (2010) (arguing that a cyber security doctrine can answer questions concerning the roles and responsibilities in cyber operations and events such as cyber attacks).

188. Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, para. 113 (June 27).

contrary to general principles of international humanitarian law reflected in treaties."[189] Not all state documents, however, have the same probative value: in *Democratic Republic of the Congo v. Uganda*, the Court dismissed the relevance of certain internal military intelligence documents because they were unsigned, unauthenticated, or lacked explanation of how the information was obtained.[190]

Military cyber documents are frequently classified in whole or in part for national security reasons.[191] According to the doctrine of privilege in domestic legal systems, litigants may refuse to submit certain evidence to a court on confidentiality grounds. No such doctrine exists before the ICJ.[192] One could actually argue that there is an obligation on the litigants to cooperate in good faith with the Court in the proceedings before it, and therefore to produce all requested documents.[193] There is, however, no sanction for failure to do so: Article 49 of the ICJ Statute limits itself to providing that "[t]he Court may, even before the hearing begins, call upon the agents to produce any document or to supply any explanations. *Formal note shall be taken of any refusal.*"[194] While the International Criminal Tribunal for the former Yugoslavia (ICTY) has found that "to grant States a blanket right to withhold, for security purposes, documents necessary for trial might jeopardise the very function of the International Tribunal, and 'defeat its essential object and purpose'."[195] The ICJ has been reluctant to draw inferences from the refusal of a party to produce confidential documents.[196] The problem has arisen twice before the Court: in the *Corfu Channel* and in the *Bosnian Genocide* cases. In the former, the ICJ called the United Kingdom, pursuant to Article 49 of the Statute, to produce an admiralty order.[197] The United Kingdom refused to produce the document on grounds of naval secrecy,[198] and witnesses also refused to answer questions in relation to the document.[199] The ICJ decided not to "draw from this refusal to produce the orders any conclusions differing from those to which the actual events gave rise."[200] In the

189. *Id.* para. 256.

190. Armed Activities on the Territory of the Congo (Dem. Rep. Congo v. Uganda), Judgment, 2005 I.C.J. 168, paras. 125, 127–28, 133–34, 137 (Dec. 19).

191. *See* Sean Lyngaas, *New Cyber Doctrine Shows More Offense, Transparency*, FCW (Oct. 24, 2014), http://fcw.com/articles/2014/10/24/cyber-offense.aspx (discussing the "past military practice of over-classifying discussions of strategy").

192. One of the problems with applying the doctrine of privilege in inter-state litigation is that international courts are unlikely to be able to verify whether state security interests are genuinely jeopardized by the document disclosure. RIDDELL & PLANT, *supra* note 54, at 208.

193. It has been observed that "when a State becomes a party to the Statute of the ICJ, it necessarily accepts the obligation to produce before the Court all evidence available to it in any case it contests." *Id.* at 49.

194. Statute of the International Court of Justice art. 49, June 26, 1945, 33 U.N.T.S. 933 (emphasis added).

195. Prosecutor v. Blaškić, Case No. IT-95-14-AR, Judgment on the Request of the Republic of Croatia for Review of the Decision of Trial Chamber II of 18 July 1997, para. 65 (Int'l Crim. Trib. for the Former Yugoslavia Oct. 29, 1997).

196. *E.g.*, Anthony Carty, *The Corfu Channel Case–And the Missing Admiralty Orders*, 3 L. & PRAC. INT'L CTS. & TRIBUNALS 1, 1 (2004) (detailing an instance in which the ICJ did not draw inferences from the failure of the Royal Navy to turn over confidential documents).

197. *Id.*

198. *Id.*

199. Benzing, *supra* note 56, at 1243.

200. Corfu Channel (U.K. v. Alb.), Judgment, 1949 I.C.J. 4, 32 (Apr. 9).

Bosnian Genocide case, even though Bosnia and Herzegovina had called upon the Court to request Serbia and Montenegro to produce certain documents classified as military secrets, the Court decided not to proceed with the request, although it reserved the right subsequently to request the documents *motu proprio*.[201] In its judgment, the ICJ limited itself to noting "the Applicant's suggestion that the Court may be free to draw its own conclusions" from the fact that Serbia and Montenegro had not produced the document voluntarily.[202] However, it does not seem that the Court ultimately drew any inferences from Serbia's non-disclosure of the classified documents.[203] It should be noted that, in both of the above-mentioned cases, alternative evidence was available to the Court.[204] It has been suggested that "it remains a matter of conjecture how the ICJ might respond in cases where a confidential communication is the only possible evidence to determine the veracity of a factual assertion, and no alternative materials are available."[205] A possible solution is that any classified information be produced in closed sittings of the court.[206]

Documents of international organizations may also be presented as evidence.[207] Overall, the Court has given particular credit to U.N. reports, Security Council resolutions, and other official U.N. documents.[208] In *Bosnian Genocide*, the ICJ stated that the probative value of reports from official or independent bodies "depends, among other things, on (1) the source of the item of evidence (for instance, partisan or neutral), (2) the process by which it has been generated (for instance an anonymous press report or the product of a careful court or court-like process), and (3) the quality of the character of the item (such as statements against interest, and agreed or uncontested facts)."[209] Several documents of international organizations address cyber issues.[210] In particular, information security has been on the U.N. agenda since 1998, when the Russian Federation introduced a draft resolution in the First Committee of the U.N. General Assembly.[211] Since then, the General Assembly has adopted a series of annual resolutions on the topic.[212] The resolutions have called for the views of the U.N. Member States on information security and established three Groups of Governmental Experts that have examined threats in cyberspace and discussed "cooperative measures to address them."[213]

---

201. Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosn. & Herz. v. Serb. & Montenegro), Judgment, 2007 I.C.J. 43, para. 44 (Feb. 26).

202. *Id.* para. 206.

203. RIDDELL & PLANT, *supra* note 53, at 214.

204. *See generally* Carty, *supra* note 196; *Bosn. & Herz. v. Serb. & Montenegro*, 2007 I.C.J. 43.

205. RIDDELL & PLANT, *supra* note 53, at 217.

206. *Id.* at 218; Benzing, *supra* note 56, at 1243.

207. *See* RIDDELL & PLANT, *supra* note 53, at 85–87.

208. Teitelbaum, *supra* note 65, at 146.

209. *Bosn. & Herz. v. Serb. & Montenegro*, 2007 I.C.J. para. 227. In the case of the "Fall of Srebrenica" Report of the Secretary-General, the Court concluded that "the care taken in preparing the report, its comprehensive sources and the independence of those responsible for its preparation all lend considerable authority to it." *Id.* para. 229–30.

210. *E.g.*, G.A. Res. 66/24, at 2, U.N. Doc. A/RES/66/24 (Dec 13, 2011) (expressing concern over "international information security").

211. *Developments in the Field of Information and Telecommunications in the Context of International Security*, U.N. OFFICE FOR DISARMAMENT AFFAIRS, http://www.un.org/disarmament/topics/informationsecurity/ [hereinafter U.N. OFFICE FOR DISARMAMENT AFFAIRS].

212. *Id.*

213. *Id.*

While the first Group, established in 2004, did not produce a substantive report,[214] the second, created in 2009, issued a report in 2010,[215] and the third Group, which met between 2012 and 2013, also adopted a final report containing a set of recommendations.[216] In addition, the views of U.N. Member States on information security are contained in the annual reports of the U.N. Secretary-General on developments in the field of information and telecommunications in the context of international security.[217]

The Court has also relied on fact-finding from commissions and other courts.[218] In *Dem. Rep. Congo v. Uganda*, the Court considered the Report of the Porter Commission, observing that neither party had challenged its credibility.[219] Furthermore, the Court accepted that "evidence [included in the Report] obtained by examination of persons directly involved, and who were subsequently cross-examined by judges skilled in examination and experienced in assessing large amounts of factual information, some of it of a technical nature, merits special attention."[220] For these reasons, facts alleged by the parties that found confirmation in the Report were considered clearly and convincingly proved.[221] There are, however, no examples of reports by judicial commissions in relation to cyber operations.[222] One can at best recall the 2009 Report of the Independent Fact-Finding Mission on the Conflict in Georgia established by the Council of the European Union,[223] which briefly addressed the cyber operations against Georgia.[224] The Report, however, is not of great probative weight, as it did not reach any conclusion on those operations' attribution or legality, simply noting that "[i]f these attacks were directed by a government or governments, it is likely that this form of warfare was used for the first time in an inter-state armed conflict."[225] Even if not of

214. U.N. Office for Disarmament Affairs, Fact Sheet: Developments in the Field of Information and Telecommunications in the Context of International Security, http://www.un.org/disarmament/HomePage/factsheet/iob/Information_Security_Fact_Sheet.pdf.

215. Grp. of Governmental Experts on Dev. in the Field of Info. and Telecomm. in the Context of Int'l Sec., Developments in the Field of Information and Telecommunications in the Context of International Security, 65th Sess., U.N. Doc. A/65/201 (July 30, 2010).

216. Grp. of Governmental Experts on Dev. in the Field of Info. and Telecomm. in the Context of Int'l Sec., Rep. of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, U.N. Doc A/68/98 (June 24, 2013).

217. *See* U.N. OFFICE FOR DISARMAMENT AFFAIRS, *supra* note 211 (collecting such annual reports).

218. Teitelbaum, *supra* note 65, at 152.

219. *Id.*; Armed Activities on the Territory of the Congo (Dem. Rep. Congo v. Uganda), 2005 I.C.J. 168, para. 60 (Dec. 19).

220. *Dem. Rep. Congo v. Uganda*, 2005 I.C.J. para. 61.

221. *See* Teitelbaum, *supra* note 65, at 153 ("It appears that when a fact alleged by one of the parties was confirmed by one of the findings of the Porter Commission, the Court accepted the evidence has having met a clear and convincing standard of proof.").

222. *See generally* Major Arie J. Schaap, *Cyber Warfare Operations: Development and Use under International Law*, 64 A.F. L. REV. 121, 121–73 (2009) (providing a holistic review of international cyber operations with no reference to judicial commission reports).

223. INDEP. INT'L FACT-FINDING MISSION ON THE CONFLICT IN GEOR., REPORT 2 (2009), http://rt.com/files/politics/georgia-started-ossetian-war/iiffmcg-volume-ii.pdf.

224. *Id.* at 217–19.

225. *Id.* at 219.

use to establish attribution, however, the Report could be relied on to establish that the cyber operations against Georgia did in fact occur.[226]

Documents produced by NGOs and think tanks may also play an evidentiary role, albeit a limited one. In relation to cyber operations, the CCD COE has prepared reports containing technical and legal discussion of the Estonia, Georgia and Iran cases, as well as of other cyber incidents.[227] Project Grey Goose produced an open source investigation into cyber conflicts, including the 2008 cyber attacks on Georgia.[228] In that case, the Report concluded "with high confidence that the Russian government will likely continue its practice of distancing itself from the Russian nationalistic hacker community thus gaining deniability while passively supporting and enjoying the strategic benefits of their actions."[229] Information security companies like Symantec, McAfee, and Mandiant also regularly compile detailed technical reports on cyber threats and specific incidents.[230] In general, however, reports from NGOs and other non-governmental bodies have been considered by the ICJ as having less probative value than publications of States and international organizations and have been used in a corroborative role only.[231] In *Democratic Republic of the Congo v. Uganda*, for instance, the ICJ considered a report by International Crisis Group not to constitute "reliable evidence."[232] Similarly, in *Oil Platforms* the Court did not find publications such as *Lloyd's Maritime Information Service*, the *General Council of British Shipping* or *Jane's Intelligence Review* to be authoritative public sources, as it had no "indication of what was the original source, or sources, or evidence on which the public sources relied."[233] This "unequal treatment" of documents of international organizations and NGOs has been criticized: "the correct approach is for the Court to apply its general evaluative criteria to documents produced by NGOs just as it does to those generated by UN actors."[234]

As far as press reports and media evidence are concerned, one may recall, in the cyber context, the above-mentioned *New York Times* articles attributing Stuxnet to the United States and Israel.[235] The ICJ, however, has been very reluctant to accept press reports as evidence and has treated them "with great caution."[236] Press reports that rely only on one source, rely on an interested source, or give no account of their

226. *See id.* at 217–19 (detailing the occurrences that point to a clear indication that cyber attacks took place against Georgia).

227. The CCD COE is a think tank based in Tallinn, Estonia that was created after the 2008 DDoS attacks against the Baltic state. *NATO Opens New Centre of Excellence on Cyber Defence*, NATO (May 14, 2008), http://www.nato.int/docu/update/2008/05-may/e0514a.html. It is not integrated into NATO's structure or funded by it. *Id.* Its reports can be accessed at https://www.ccdcoe.org/publications.html.

228. *See generally* PROJECT GRAY GOOSE, *supra* note 140.

229. *Id.* at 3.

230. *See, e.g.*, MANDIANT, APT1, *supra* note 30, at 1–74 (compiling one such report about China's cyber espionage unit).

231. RIDDELL & PLANT, *supra* note 53, at 249.

232. Armed Activities on the Territory of the Congo (Dem. Rep. Congo v. Uganda), Judgment, 2005 I.C.J. 168, para. 129 (Dec. 19).

233. Oil Platforms (Iran v. U.S.), Judgment, 2003 I.C.J. 161, para. 60 (Nov. 6).

234. RIDDELL & PLANT, *supra* note 53, at 250.

235. *See supra* text accompanying notes 18–21.

236. Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, para. 62 (June 27).

sources have therefore been treated as having no probative value.[237] In the *Bosnian Genocide* case, the Court dismissed an article in *Le Monde*, qualifying it as "only a secondary source."[238] In *Nicaragua*, the Court held that, even when they meet "high standards of objectivity," it would regard the reports in press articles and extracts from books presented by the parties "not as evidence capable of proving facts, but as material which can nevertheless contribute, in some circumstances, to corroborating the existence of a fact, i.e., as illustrative material additional to other sources of evidence."[239] This was dependent on the sources being "wholly consistent and concordant as to the main facts and circumstances of the case."[240] It has been suggested that this expression means that "the press reports in question would have to confirm the facts as alleged by both of the parties, or confirm facts that have not been denied or contested by the parties."[241]

Apart from this, press reports may contribute, together with other sources, to demonstrate public knowledge of facts of which the Court may take judicial notice, thus relieving a party from having to discharge the burden of proof with regard to those facts.[242] The fact that cyber incidents like Stuxnet have received extensive media coverage—and that the *New York Times* article has been followed by many others, including in *The Washington Post*[243]—would not, however, as such increase their probative weight or mean that the covered facts are of public knowledge.[244] As already mentioned, in *Nicaragua* the ICJ noted that "[w]idespread reports of a fact may prove on closer examination to derive from a single source, and such reports, however numerous, will in such case have no greater value as evidence than the original source."[245]

B. Official Statements

Statements made by official authorities outside the context of the judicial proceedings may play an important evidentiary role. In the *Tehran Hostages* case, for instance, the ICJ recalled that it had "a massive body of information from various sources concerning the facts and circumstances of the present case, including numerous official statements of both Iranian and United States authorities."[246]

---

237. *Dem. Rep. Congo v. Uganda*, 2005 I.C.J. para. 68.

238. Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosn. & Herz. v. Serb. & Montenegro), Judgment, 2007 I.C.J. 43, para. 357 (Feb. 26).

239. *Nicar. v. U.S.*, 1986 I.C.J. para. 62.

240. *Dem. Rep. Congo v. Uganda*, 2005 I.C.J. para. 68 (citing United States Diplomatic and Consular Staff in Tehran (U.S. v. Iran), Judgment, 1980 I.C.J. 3, para. 13 (May 24))

241. Teitelbaum, *supra* note 65, at 140.

242. *Nicar. v. U.S.*, 1986 I.C.J. para. 63.

243. *See* Ellen Nakashima, Greg Miller & Julie Tate, *U.S., Israel Developed Flame Computer Virus to Slow Iranian Nuclear Efforts, Officials Say*, WASH. POST, June 19, 2012, http://www.washingtonpost.com/world/national-security/us-israel-developed-computer-virus-to-slow-iranian-nuclear-efforts-officials-say/2012/06/19/gJQA6xBPoV_story.html (discussing the similarities between Stuxnet and the sophisticated virus known as "Flame").

244. *See, e.g., Nicar. v. U.S.*, 1986 I.C.J. para. 63 (explaining that extensive reports and coverage do not necessarily provide probative evidentiary weight).

245. *Id.*

246. United States Diplomatic and Consular Staff in Tehran (U.S. v. Iran), Judgment, 1980 I.C.J. 3, para. 13 (May 24).

Statements "emanating from high-ranking official political figures, sometimes indeed of the highest rank, are of particular probative value when they acknowledge facts or conduct unfavourable to the State represented by the person who made them."[247] However, all depends on how those statements were made public: "evidently, [the Court] cannot treat them as having the same value irrespective of whether the text is to be found in an official national or international publication, or in a book or newspaper."[248] In other words, statements that can be directly attributed to a state are of more probative value.

The U.S. Department of Defense's *Assessment of International Legal Issues in Information Operations* confirms that "[s]tate sponsorship might be persuasively established by such factors as . . . public statements by officials."[249] There does not seem to be, however, any official statement by Russian or Chinese authorities directly or even indirectly acknowledging responsibility for the cyber operations against Estonia, Georgia, and the United States; on the contrary, involvement was denied.[250] With regard to Stuxnet, U.S. and Israeli authorities neither admitted nor denied attribution when asked questions about the incident.[251] Whether this allows inferences to be drawn is discussed below.[252]

C. *Witness Testimony*

Witnesses may be called to provide direct oral evidence by the Court and by the litigants: The latter case is conditioned upon the absence of objections by the other litigant or the recognition by the Court that the evidence is likely to be relevant.[253] The Court may also put questions to the witnesses and experts called by the parties.[254] The ICJ has not made extensive use of oral evidence.[255] In *Corfu Channel*, for instance, naval officers were called to testify by the United Kingdom about the damage suffered by the Royal Navy ships and the nature and origin of the mines.[256] Albania also called witnesses to testify to the absence of mines in the Channel.[257] Nicaragua called five witnesses to testify in the *Nicaragua* case.[258] In the same case,

247. *Nicar. v. U.S.*, 1986 I.C.J. para. 64.

248. *Id.* para. 65.

249. U.S. DEP'T OF DEF., AN ASSESSMENT OF INTERNATIONAL LEGAL ISSUES IN INFORMATION OPERATIONS 21 (1999), http://www.au.af.mil/au/awc/awcgate/dod-io-legal/dod-io-legal.pdf [hereinafter ASSESSMENT OF INTERNATIONAL LEGAL ISSUES].

250. *See, e.g.*, Klimburg, *supra* note 12, at 41–42 (discussing Russian and Chinese involvement in cyber warfare and plausible deniability of such actions).

251. Richmond, *supra* note 21, at 855; Williams, *supra* note 28.

252. *See infra* Part V (discussing possible inferences).

253. Rules of Court, arts. 62(2), 63, 1978 I.C.J. Acts & Docs. 6. It should be recalled that international courts and tribunals do not normally have the authority or the capability to issue *subpoena* to coercively bring a witness before them. Wolfrum, *supra* note 36, at 560.

254. Rules of Court, art. 65, 1978 I.C.J. Acts & Docs. 6.

255. See the cases in Aguilar Mawdsley, *supra* note 79, at 543.

256. Corfu Channel (U.K. v. Alb.), Judgment, 1949 I.C.J. 4, 7–8, 10 (Apr. 9).

257. *Id.* at 11.

258. Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, para. 13 (June 27).

the Court noted that "testimony of matters not within the direct knowledge of the witness, but known to him only from hearsay" is not "of much weight."[259]

It is worth recalling that the Court has also accepted witness evidence given in written form and attached to the written pleadings, but it has treated it "with caution"[260] and has generally considered it of a probative value inferior to that of direct oral witness testimony.[261] Factors to be considered in assessing the probative weight of affidavits include time, purpose and context of production, whether they were made by disinterested witnesses, and whether they attest to the existence of facts or only refer to an opinion with regard to certain events.[262]

D. Enquiry and Experts

According to Article 50 of the ICJ Statute, "[t]he Court may, at any time, entrust any individual, body, bureau, commission, or other organization that it may select, with the task of carrying out an enquiry or giving an expert opinion."[263] Enquiries have never been commissioned by the Court, which has rather relied on fact-finding reports from other sources.[264] Experts may be necessary in cases of a highly technical nature or that involve expertise not possessed by the judges.[265] It is likely, therefore, that the Court will appoint experts in cases involving cyber technologies. The Court, however, would not be bound by their report.

The parties may also call experts.[266] As to the form of their participation in the oral proceedings, in *Pulp Mills* the ICJ reminded the parties that:

> [T]hose persons who provide evidence before the Court based on their scientific or technical knowledge and on their personal experience should testify before the Court as experts, witnesses or in some cases in both capacities, rather than counsel, so that they may be submitted to questioning by the other party as well as by the Court.[267]

In the *Whaling in the Antarctic* case, therefore, the experts called by both Australia and Japan gave evidence as expert witnesses and were cross-examined,[268] and the Court relied heavily on their statements to conclude that the special permits granted

259. *Id.* para. 68.

260. Territorial and Maritime Dispute Between Nicaragua and Honduras in the Caribbean Sea (Nicar. v. Hond.), Judgment, 2007 I.C.J. 659, para. 244 (Oct. 8).

261. *See* RIDDELL & PLANT, *supra* note 53, at 280–81 (noting the Court's "similar view of the inferiority of affidavit evidence relative to direct witness testimony").

262. *Nicar. v. Hond.*, 2007 I.C.J. para. 244.

263. Statute of the International Court of Justice art. 50, June 26, 1945, 33 U.N.T.S. 933.

264. Benzing, *supra* note 56, at 1259. For criticism of this practice, see Joyce, *supra* note 68, at 283 (calling for reform of fact-finding processes for the ICJ).

265. In the *Corfu Channel* Case, the Court appointed a Committee of Experts because of the insurmountable differences of opinion between the parties on certain facts. Corfu Channel (U.K. v. Alb.), 1949 I.C.J. 4, 9 (Apr. 9).

266. Rules of Court, art. 63, 1978 I.C.J. Acts & Docs. 6.

267. Pulp Mills on the River Uruguay (Arg. v. Uru.), Judgment, 2010 I.C.J. 14, para. 167 (Apr. 20).

268. Whaling in the Antarctic (Aust. v. Japan: N.Z. intervening), Judgment, 2014 I.C.J. 148, paras. 20–21 (Mar. 31).

by Japan for the killing, taking, and treatment of whales had not been granted "for purposes of scientific research."[269]

E. Digital Evidence

Digital forensics "deals with identifying, storing, analyzing, and reporting computer finds, in order to present valid digital evidence that can be submitted in civil or criminal proceedings."[270] It includes the seizure, forensic imaging, and analysis of digital media, and the production of a report on the evidence so collected.[271] It seems that most countries "do not make a legal distinction between electronic evidence and physical evidence. While approaches vary, many countries consider this good practice, as it ensures fair admissibility alongside all other types of evidence."[272] Of course, not only do data have to be collected, but they also need to be interpreted, and the parties may disagree on their interpretation.

For several reasons, however, digital evidence on its own is unlikely to play a decisive role in establishing state responsibility for cyber operations. First, digital evidence is "volatile, has a short life span, and is frequently located in foreign countries."[273] Second, the collection of digital evidence can be very time consuming and requires the cooperation of the relevant internet service providers, which may be difficult to obtain when the attack originates from other States.[274] Third, although digital evidence may lead to the identification of the computer or computer system from which the cyber operation originates, it does not necessarily identify the individual(s) responsible for the cyber operation (as the computer may have been hijacked, or the IP spoofed).[275] In any case, such digital evidence will say nothing about whether the conduct of those individuals can be attributed to a State under the law of state responsibility.[276]

---

269. *See id.* para. 227.

270. PRESIDENCY OF THE COUNCIL OF MINISTERS, NATIONAL STRATEGIC FRAMEWORK FOR CYBERSPACE SECURITY 42 (2013), *available at* http://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/italian-national-strategic-framework-for-cyberspace-security.pdf.

271. *See* Jay P. Kesan & Carol M. Hayes, *Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace*, 25 HARV. J.L. & TECH. 429, 482 (2012) (describing traceback technology as a way to "identify the source of the attack"); U.S. DEP'T OF DEF., DEPARTMENT OF DEFENSE CYBERSPACE POLICY REPORT: A REPORT TO CONGRESS PURSUANT TO THE NATIONAL DEFENSE AUTHORIZATION ACT FOR FISCAL YEAR 2011, Section 9344 (2011) *available at* http://www.defense.gov/home/features/2011/0411_cyberstrategy/docs/NDAA%20Section %20934%20Report_For%20webpage.pdf (discussing ways the U.S. Department of Defense is seeking to improve attribution capabilities through behavior-based algorithms).

272. U.N. OFFICE ON DRUGS AND CRIME, COMPREHENSIVE STUDY ON CYBERCRIME: DRAFT—FEBRUARY 2013, xxiv (2013), *available at* http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/ CYBERCRIME_STUDY_210213.pdf.

273. Fred Schreier, *On Cyberwarfare* 65 (DCAF Horizon 2015, Working Paper No. 7, 2012).

274. *Id.* at 46.

275. *Id.* at 65.

276. *Cf.* TALLINN MANUAL r. 6–7 (noting various ways in which a State might be held responsible for cyber action taken by State and non-state actors).

V. PRESUMPTIONS AND INFERENCES IN THE CYBER CONTEXT

As Judge ad hoc Franck emphasized in *Sovereignty over Pulau Ligitan and Pulau Sipadan*, "[p]resumptions are necessary and well-established aspects both of common and civil law and cannot but be a part of the fabric of public international law."[277] Previously, in his dissenting opinion in *Corfu Channel*, Judge Azevedo had argued that "[i]t would be going too far for an international court to insist on direct and visual evidence and to refuse to admit, after reflection, a reasonable amount of human presumptions with a view to reaching that state of moral, human certainty with which, despite the risk of occasional errors, a court of justice must be content."[278]

Although the difference is often blurred in inter-state litigation, presumptions may be prescribed by law (legal presumptions, or presumptions of law), or be reasoning tools used by the judges (presumptions of fact, or inferences).[279] In other words, "[p]resumptions of law derive their force from *law*, while presumptions of fact derive their force from *logic*."[280] In international law, presumptions of law can derive from treaties, international customs, and general principles of law.[281] According to Judge Owada in his dissenting opinion in the *Whaling in the Antarctic* case, for instance, good faith on the part of a contracting State in performing its obligations under a treaty "has necessarily to be presumed,"[282] although the presumption is subject to rebuttal.[283]

Inferences, or presumptions of fact, are closely linked to circumstantial evidence.[284] In the *Corfu Channel* case, Judge Padawi Pasha defined circumstantial evidence as "facts which, while not supplying immediate proof of the charge, yet make the charge problable [sic] with the assistance of reasoning."[285] Inferences "convincingly" establishing state sponsorship for cyber operations are suggested in the U.S. Department of Defense's *Assessment of International Legal Issues in Information Operations*, including "the state of relationships between the two countries, the prior involvement of the suspect State in computer network attacks,

277. Sovereignty over Pulau Ligitan & Pulau Sipadan (Indon./Malay.), Judgment, 2002 I.C.J. 691, para. 44 (Dec. 17) (dissenting opinion of Judge ad hoc Franck).

278. Corfu Channel (U.K. v. Alb.), Judgment, 1949 I.C.J. 4, 90–91 (Apr. 9) (dissenting opinion of Judge Azevedo).

279. *See* C.F. Amerasinghe, *Presumptions and Inferences in Evidence in International Litigation*, 3 L. & PRAC. INT'L CTS. & TRIBUNALS 395, 395 (2004) (distinguishing irrebuttable presumptions (*juris et de jure*) from rebuttable ones (*juris tantum*) because the former are immune to evidence proving facts that contradict them, while the latter shift the burden of demonstrating the opposite to the other litigant).

280. Thomas M. Franck & Peter Prows, *The Role of Presumptions in International Tribunals*, 4 L. & PRAC. INT'L CTS. & TRIBUNALS 197, 203 (2005) (internal citations omitted).

281. MOJTABA KAZAZI, BURDEN OF PROOF AND RELATED ISSUES: A STUDY ON EVIDENCE BEFORE INTERNATIONAL TRIBUNALS 245 (1996).

282. Whaling in the Antarctic (Austl. v. Japan: N.Z. intervening), Judgment, 2014 I.C.J. 148, para. 21 (Mar. 31) (dissenting opinion of Judge Owada).

283. *Id.* para. 42.

284. RIDDELL & PLANT, *supra* note 53, at 113; *see also* Barcelona Traction, Light and Power Company, Limited. (Belg. v. Spain), 1964 I.C.J. 6, 80 (July 24) (separate opinion of Judge Bustamante) ("[It may] be possible to arrive at a conclusion on the basis merely of inferences or deductions forming part of a logical process . . . .").

285. Corfu Channel (U.K. v. Alb.), Judgment, 1949 I.C.J. 4, 59 (Apr. 9) (dissenting opinion of Judge Pasha).

the nature of the systems attacked, the nature and sophistication of the methods and equipment used, the effects of past attacks, and the damage which seems likely from future attacks."[286] In its reply to the U.N. Secretary-General on issues related to information security, the United States also claimed that "the identity and motivation of the perpetrator(s) can only be inferred from the target, effects and other circumstantial evidence surrounding an incident."[287] The commentary to Rule 11 of the *Tallinn Manual* refers to inferences from "the prevailing political environment, whether the . . . operation portends the future use of military force, the identity of the attacker, any record of cyber operations by the attacker, and the nature of the target (such as critical infrastructure)," in order to determine whether a cyber operation qualifies as a use of force under Article 2(4) of the U.N. Charter.[288]

The ICJ, however, "has demonstrated an increasing resistance to the drawing of inferences from secondary evidence."[289] Only inferences to protect state sovereignty are normally drawn by the Court, while others are treated with great caution.[290] The ICJ has drawn inferences in situations such as exclusive control of territory and non-production of documents.[291] As to the first, it has been argued that the State from which the cyber operation originates has presumptive knowledge of such operation. U.S. officials have claimed, for instance, that, with the control that the Iranian government exercises over the internet, it is "hard to imagine" that cyber attacks originating from Iran against U.S. oil, gas, and electricity companies could be conducted without governmental knowledge, even in the absence of direct proof of state involvement.[292] The same considerations may be extended to cyber operations originating from China and other States where access to the Internet is under strict governmental control. The U.S. Department of Defense's *Assessment of International Legal Issues in Information Operations* also claims that "[s]tate sponsorship might be persuasively established by such factors as . . . the location of the offending computer within a state-controlled facility."[293] In literature, Richard Garnett and Paul Clarke have claimed that "in a situation where there have been

286. ASSESSMENT OF INTERNATIONAL LEGAL ISSUES, *supra* note 249, at 21–22. For a critique of the use of the sophistication criterion to establish attribution, see generally Clement Guitton and Elaine Korzak, *The Sophistication Criterion for Attribution: Identifying the Perpetrators of Cyber-Attacks*, 158 RUSI J. 62 (2013).

287. *Developments in the Field of Information and Telecommunications*, *supra* note 3, at 16; *see also* DEP'T OF INFO. TECH., GOV'T OF INDIA, DISCUSSION DRAFT ON NATIONAL CYBER SECURITY POLICY 4 (2011) [hereinafter DISCUSSION DRAFT ON NATIONAL CYBER SECURITY POLICY], *available at* http://deity.gov.in/sites/upload_files/ dit/files/ncsp_060411.pdf ("The origin, identity of the perpetrator, or motivation for the disruption can be difficult to ascertain. Often, the perpetrators of these activities can only be inferred from the target, the effect or other circumstantial evidence.").

288. TALLINN MANUAL r. 11 cmt. 10.

289. Teitelbaum, *supra* note 74, at 157.

290. RIDDELL & PLANT, *supra* note 54, at 413.

291. Waxman has highlighted the need to use "propensity inferences", which are based on the past behavior of a regime and its inclination to undertake certain actions. Waxman, *supra* note 57, at 66. He concludes that "there is no escaping some reliance on propensity inferences because of the limits of forensic evidence." *Id.* at 68. As the author himself points out, however, previous conduct can be misleading when the regime in question bluffs about its capabilities to intimidate or deter, as in the case of Saddam Hussein's Iraq. *Id.*

292. Nicole Perlroth & David E. Sanger, *New Computer Attacks Traced to Iran, Officials Say*, N.Y. TIMES, May 24, 2013, http://www.nytimes.com/2013/05/25/world/middleeast/new-computer-attacks-come-from-iran-officials-say.html?_r=0.

293. ASSESSMENT OF INTERNATIONAL LEGAL ISSUES, *supra* note 249, at 21.

repeated instances of hostile computer activity emanating from a State's territory directed against another State, it seems reasonable to presume that the host State had knowledge of such attacks and so should incur responsibility."[294] At least some cyber attacks against Estonia and Georgia originated from Russian IP addresses, including those of state institutions.[295] The Mandiant Report also traced the cyber intrusions into U.S. computers back to Chinese IP addresses.[296] As has been seen, however, in the *Corfu Channel* case the ICJ held that "it cannot be concluded from the mere fact of the control exercised by a State over its territory . . . that that State necessarily knew, or ought to have known, of any unlawful act perpetrated therein . . . ."[297] Only if there are other indications of state involvement may territorial control contribute to establish knowledge.[298] In *Oil Platforms*, the ICJ also refused to accept the US argument that the territorial control exercised by Iran over the area from which the missile against the *Sea Isle City* had been fired was sufficient to demonstrate Iran's responsibility.[299] These conclusions are transposed in the cyber context by Rules 7 and 8 of the *Tallinn Manual*, according to which neither the fact that a cyber operation originates from a State's governmental cyber infrastructure nor that it has been routed through the cyber infrastructure located in a State are sufficient evidence for attributing the operation to those States, although it may be "an indication that the State in question is associated with the operation."[300] The *Tallinn Manual* does not clarify what probative value this "indication" would have.

If control of cyber infrastructure is not on its own sufficient to prove knowledge of the cyber operations originating therefrom, much less direct attribution, it may however have "a bearing upon the methods of proof available to establish the knowledge of that State as to such events."[301] In particular,

> [b]y reason of this exclusive control [within its frontiers], the other State, the victim of a breach of international law, is often unable to furnish direct proof of facts giving rise to responsibility. Such a State should be allowed a *more liberal recourse to inferences of fact and circumstantial evidence.* This indirect evidence is admitted in all systems of law, and its use is recognized by international decisions.[302]

---

294. Richard Garnett & Paul Clarke, *Cyberterrorism: A New Challenge for International Law*, *in* ENFORCING INTERNATIONAL LAW NORMS AGAINST TERRORISM 465, 479 (Andrea Bianchi ed., 2004).

295. U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES, *supra* note 8, at 173; TIKK ET AL., *supra* note 14, at 75.

296. MANDIANT, APT 1, *supra* note 3030, at 4.

297. Corfu Channel (U.K. v. Alb.), Judgment, Merits, 1949 I.C.J. 4, 18 (Apr. 9). *See contra id.* at 44 (separate opinion of Judge Alvarez) ("[E]very State is considered as having known, or as having a *duty* to have known, of prejudicial acts committed in parts of its territory where local authorities are installed . . . .").

298. *See U.K. v. Alb.*, 1949 I.C.J. at 18 ("[T]he fact of this exclusive territorial control exercised by a State within its frontiers has a bearing on the methods of proof available to establish the knowledge of that State as to such events.").

299. Oil Platforms (Iran v. U.S.), Judgment, 2003 I.C.J. 161, para. 61 (Nov. 6).

300. TALLINN MANUAL r. 7.

301. *U.K. v. Alb.*, 1949 I.C.J. at 18.

302. *Id.* (emphasis added).

According to the Court, then, inferences become particularly valuable, and assume a probative value higher than normal, when a litigant is unable to provide direct proof of facts because the evidence is under the exclusive territorial control of the other litigant.[303] Such indirect evidence "must be regarded as of special weight when it is based on a series of facts linked together and leading logically to a single conclusion."[304] The ICJ, therefore, coupled the exclusive territorial control by Albania with its silence about the mine laying and other circumstantial evidence, and concluded that Albania had knowledge of the mines.[305] Transposed to the cyber context, the presence or origination of the hazard in the cyber infrastructure controlled by a State does not per se demonstrate knowledge by that State, but may contribute to such a finding if it is accompanied by other circumstantial evidence pointing in that direction. In *Corfu Channel*, however, the Court specified that, when proof is based on inferences, these must "leave *no room* for reasonable doubt."[306] In the *Bosnian Genocide* case, the Court confirmed that in demonstrating genocidal intent "for a pattern of conduct to be accepted as evidence of its existence, it would have to be such that it could only point to the existence of such intent."[307] In any case, "no inference can be drawn which is inconsistent with facts incontrovertibly established by the evidence."[308]

Of course, the Court will first have to determine whether the party has "exclusive territorial control"[309] of the cyber infrastructure from which the cyber operations originated (and, therefore, potentially of the evidence of who was responsible for them) before allowing the more liberal recourse to inferences. This may cause particular difficulties in cases of armed conflict: In the *DRC v. Uganda* case, for instance, one of the issues in dispute was whether Uganda had had control over Congolese territory.[310] In the cyber context, determining whether a litigant has "territorial control" of the cyber infrastructure, and whether such control is "exclusive" may be equally difficult to establish and is linked to the ongoing debate on the States' creeping jurisdiction over the Internet and cyberspace in general.[311] In this context, it should be recalled that Rule 1 of the *Tallinn Manual* accepts that "[a] State may exercise control over cyber infrastructure and activities within its sovereign territory."[312]

It should also be noted that the ICJ has not always allowed the "more liberal recourse to inferences of fact and circumstantial evidence" in cases of exclusive

303. *Id.*

304. *Id.* This may, for instance, be the case when a large number of cyber operations originate from the governmental cyber infrastructure of the same country.

305. *Id.* at 22.

306. *U.K. v. Alb.*, 1949 I.C.J. at 18.

307. Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosn. & Herz. v. Serb. & Montenegro), Judgment, 2007 I.C.J. 43, para. 373 (Feb. 26).

308. Temple of Preah Vihear (Cambodia v. Thai.), Judgment, 1962 I.C.J. 39, 109 (June 15) (separate opinion of Sir Spender).

309. *See* Waxman, *supra* note 57, at 72 (discussing situations when shifting the burden of proof may be acceptable under ICJ precedent, such as *Corfu Channel*, in which the party in "exclusive territorial control" inhibits the discovery of evidence).

310. Armed Activities on the Territory of the Congo (Dem Rep. Congo v. Uganda), Judgment, 2005 I.C.J. 168, para. 167–69.

311. *See* ROSCINI, *supra* note 1, 23–24 (discussing the difficulty in extending "existing rules and principles to . . . cyber operations").

312. TALLINN MANUAL r. 1.

territorial control.[313] In the *Bosnian Genocide* case, Bosnia and Herzegovina argued that, because of Serbia and Montenegro's geographical situation, the standard of proof should be lower, and that the respondent "had a special duty of diligence in preventing genocide and the proof of its lack of diligence can be inferred from fact and circumstantial evidence."[314] The Court rejected this reasoning and established Serbia and Montenegro's responsibility for failure to prevent genocide not on the basis of inferences but on documentary evidence and ICTY testimony.[315]

Does refusal to disclose evidence allow negative inferences? Article 38 of the Rules of Procedure of the Inter-American Commission on Human Rights provides that the facts alleged in the petition "shall be presumed to be true if the State has not provided responsive information during the period set by the Commission under the provisions of Article 37 of these Rules of Procedure, as long as other evidence does not lead to a different conclusion."[316] This is due to the different nature of human rights tribunals, where one of the parties is an individual and the other is a government, while disputes before the ICJ are between sovereign states.[317] According to Article 49 of its Statute, the ICJ may only take "[f]ormal note" of the refusal to disclose evidence: This provision authorizes the Court to draw inferences but does not create a presumption of law.[318] In any case, as has already been seen, in the *Corfu Channel* and the *Bosnian Genocide* cases the Court declined to draw any inferences from refusal to produce evidence, in the former case because there was a series of facts contrary to the inference sought.[319] Of course, if the litigant decides not to produce certain evidence, it will bear the risk that the facts it claims will not be considered sufficiently proved.[320]

VI. INADMISSIBLE EVIDENCE

There are no express rules on the admissibility of evidence in the ICJ Statute. Therefore, "[t]he general practice of the Court has been to admit contested documents and testimony, subject to the reservation that the Court will itself be the judge of the weight to be accorded to it."[321] Evidence may, however, be declared

313. Corfu Channel (U.K. v. Alb.), Judgment, 1949 I.C.J. 4, 18 (Apr. 9).

314. Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosn. & Herz. v. Fed. Rep. Yugo), Reply of Bosnia and Herzegovina, para. 22 (Apr. 23, 1998).

315. *See* Teitelbaum, *supra* note 74, at 138–39 (analyzing Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosn. & Herz. v. Serb. & Montenegro), Judgment, 2007 I.C.J. 43, para. 242 (Feb. 26)). For critical comments on the ICJ's reliance on ICTY evidence, see Joyce, *supra* note 68, 298–305.

316. R.P. Inter-Am. Comm'n H.R. art. 38 (2009).

317. *Compare* Jo M. Pasqualucci, *Advisory Practice of the Inter-American Court of Human Rights: Contributing to the Evolution of International Human Rights Law*, 38 STAN. J. INT'L L. 241, 242 (2002) (emphasizing international law rules favorable to the individual in human rights cases), *with* 48 C.J.S. International Law § 61 (describing the differing nature of the ICJ).

318. Statute of the International Court of Justice art. 49, June 26, 1945, 33 U.N.T.S. 933.

319. *See, e.g.*, Corfu Channel (U.K. v. Alb.), Judgment, 1949 I.C.J. 4, 32 (Apr. 9) (explaining the Court's determination that it cannot draw conclusions from the United Kingdom's refusal to produce documents XCU).

320. Statute of the International Court of Justice art. 49, June 26, 1945, 33 U.N.T.S. 933.

321. Keith Highet, *Evidence, the Court, and the Nicaragua Case*, 81 AM. J. INT'L L. 1, 13 (1987).

inadmissible because it has been produced too late or not in the prescribed form.[322] Another example of inadmissible evidence is provided by the decision of the Permanent Court of International Justice in the *Factory at Chorzów* case, where the ICJ's predecessor held that it "cannot take account of declarations, admissions or proposals which the Parties may have made in the course of direct negotiations [when] . . . the negotiations in question have not . . . led to an agreement between [the parties]."[323] The underlying reason for the inadmissibility of such material is to facilitate the diplomatic settlement of international disputes through negotiations, so that the negotiating parties do not have to fear that what they say in the negotiating context may be used against them in subsequent judicial proceedings.[324]

Is evidence obtained through a violation of international law also inadmissible? Traditional espionage and cyber exploitation, used in support of traceback technical tools, may be a helpful instrument to establish proof of state responsibility for cyber operations.[325] India has noted that "[c]yber security intelligence forms an integral component of security of cyber space in order to be able to anticipate attacks, adopt suitable counter measures and attribute the attacks for possible counter action."[326] It is doubtful whether the above activities constitute internationally wrongful acts, although one commentator has argued, for instance, that cyber espionage may be a violation of the sovereignty of the targeted State whenever it entails an unauthorized intrusion into cyber infrastructure located in another State (be it governmental or

322. Statute of the International Court of Justice art. 52, June 26, 1945, 33 U.N.T.S. 933. Late evidence may be admissible if the other litigant consents to it or if the Court does not reject it. Christian J Tams, *Article 52*, *in* THE STATUTE OF THE INTERNATIONAL COURT OF JUSTICE: A COMMENTARY, *supra* note 56, at 1312–16.

323. Factory at Chorzów (Ger. v. Pol.), Claim for Indemnity, 1927 P.C.I.J. (ser. A) No. 9, at 19. The ICJ referred to this limit in Frontier Dispute (Burk. Faso/Mali), Judgment, 1986 I.C.J. 554, para. 147 (Dec. 22); Maritime Delimitation and Territorial Questions between Qatar and Bahrain (Qatar v. Bahr.), Judgment, 1994 I.C.J. 112, para. 40 (July 1).

324. Benzing, *supra* note 56, at 1242.

325. *See* Nicholas Tsagourias, *Cyber Attacks, Self-Defence and the Problem of Attribution*, 17 J. CONFLICT & SEC. L. 229, 234 (2012) ("[I]n addition to technical investigation, intelligence and information analysis is needed in order to profile the authors of the attack . . . ."); U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES, *supra* note 8, at 140–41 ("All-source attribution takes into account whatever information is available from efforts at technical attribution, but also uses information from other sources to arrive at a judgment.").

326. *See* DISCUSSION DRAFT ON NATIONAL CYBER SECURITY POLICY, *supra* note 287, at 4.

private).[327] Data monitoring and interceptions may also be a violation of international human rights law.[328]

Assuming, *arguendo*, that espionage and cyber exploitation are, at least in certain instances, internationally wrongful acts, what is the probative value of the evidence so collected? There is no express rule in the Statute of the ICJ providing that evidence obtained through a violation of international law is inadmissible.[329] It is also not a general principle of law, as it seems to be a rule essentially confined to the U.S. criminal system.[330] As Thirlway argues, the rule in domestic legal systems is motivated by the need to protect the defendant against the wider powers of the prosecutor and its possible abuses: In inter-state litigation, there is no criminal trial and no dominant party, as the litigants are States in a position of sovereign equality.[331] In the *Corfu Channel* case, the ICJ did not dismiss evidence illegally obtained by the United Kingdom in Operation Retail; on the contrary, it relied on it in order to determine the place of the accident and the nature of the mines.[332] In fact, Albania never challenged the admissibility of the evidence acquired by the British Navy,[333] and the Court did not address the question.[334] What it found was not that the evidence had been illegally obtained, but that the purpose of gathering evidence did not exclude the illegality of certain conduct.[335] In general,

> the approach of the Court is to discourage self-help in the getting of evidence involving internationally illicit acts, not by seeking to impose

---

327. *See* Wolff Heintschel von Heinegg, *Territorial Sovereignty and Neutrality in Cyberspace*, 89 INT'L L. STUD. 123, 129 (2013) ("It could be argued . . . that damage is irrelevant and the mere fact that a State has intruded into the cyber infrastructure of another State should be considered an exercise of jurisdiction on foreign territory, which always constitutes a violation of the principle of territorial sovereignty."); *see also* ASSESSMENT OF INTERNATIONAL LEGAL ISSUES, *supra* note 249, at 19–20 ("An unauthorized electronic intrusion into another nation's computer systems may very well end up being regarded as a violation of the victim's sovereignty. It may even be regarded as equivalent to a physical trespass into a nation's territory, but such issues have yet to be addressed in the international community.... If an unauthorized computer intrusion can be reliably characterized as intentional and it can be attributed to the agents of another nation, the victim nation will at least have the right to protest, probably with some confidence of obtaining a sympathetic hearing in the world community."); Louise Doswald-Beck, *Some Thoughts on Computer Network Attack and the International Law of Armed Conflict*, 76 INT'L L. STUD. 163, 172 (2002) (arguing that, when the individual conducts intelligence gathering from outside the adversary's territory through cyber exploitation, "the situation should be no different from someone gathering data from a spy satellite").

328. *See* Jann K. Kleffner & Heather A. Harrison Dinniss, *Keeping the Cyber Peace: International Legal Aspects of Cyber Activities in Peace Operations*, 89 INT'L L. STUD. 512, 512–13 (2013).

329. RIDDELL & PLANT, *supra* note 53, at 158.

330. Hugh Thirlway, *Dilemma or Chimera?—Admissibility of Illegally Obtained Evidence in International Adjudication*, 78 AM. J. INT'L L. 622, 627–28 (1984); Nasim Hasan Shah, *Discovery by Intervention: The Right of a State to Seize Evidence Located Within the Territory of the Respondent State*, 53 AM. J. INT'L L. 595, 607–09 (1959). *Contra* Wolfrum, *supra* note 36, at 563 (stating that evidence obtained in violation of substantive international law could be inadmissible under the ICTY rules).

331. Thirlway, *supra* note 330, at 628–29.

332. Corfu Channel (U.K. v. Alb.), Judgment, 1949 I.C.J. 4, 14–15 (Apr. 9); Shah, *supra* note 330, at 606–07.

333. Thirlway, *supra* note 330, at 632.

334. *Id.*

335. *See U.K. v. Alb.*, 1949 I.C.J. at 34–35 (holding that the United Kingdom's theory of intervention with the purpose of obtaining evidence "might easily lead to perverting the administration of international justice itself.").

> any bar on the employment of evidence so collected, but by making it clear that such illicit activity is not necessary, since secondary evidence will be received and treated as convincing in appropriate circumstances.[336]

In a cyber context, this means that while litigants are not entitled to access direct evidence that is located in another State's computers or networks without authorization to submit it in the proceedings, that evidence's existence allows the court to give more weight to circumstantial evidence.[337]

CONCLUSIONS

The following main conclusions can be drawn from the application to cyber operations of the ICJ's rules and case law on evidence:

-The burden of proof does not shift in the cyber context and continues to rest on the party that alleges a certain fact.

-Whilst it is uncertain that a uniform standard of proof applicable to *all* cases involving international responsibility for cyber operations can be identified, it appears that claims of self-defense against cyber operations, like those against kinetic attacks, must be proved with clear and convincing evidence. On the other hand, fully conclusive evidence is needed to prove that a litigant conducted cyber operations amounting to international crimes, and a slightly less demanding standard seems to apply when what needs to be proved is that the State did not exercise due diligence to stop its cyber infrastructure from being used by others to commit international crimes.

-The Court may take 'formal note' of the refusal of a party to present classified cyber documents, but it has so far refrained from drawing negative inferences from the non-production of documents. In any case, any such negative inferences could not contradict factual conclusions based on consistent evidence produced by the parties.

-The Court gives more probative weight to official documents of States and international organizations such as the United Nations. NGO reports and press articles on cyber incidents are only secondary sources of evidence that may be useful to corroborate other sources or to establish the public knowledge of certain facts, providing they are sufficiently rigorous and only when they are "wholly consistent and concordant as to the main facts and circumstances of the case."[338]

-The drawing of inferences is approached by the ICJ with great caution. When there are objective difficulties for a litigant to discharge the burden of proof because the direct evidence lies within the exclusive territorial control of the other litigant, including its cyber infrastructure, a more liberal recourse to inferences of fact is admissible providing that they leave no room for reasonable doubt.

---

336. Thirlway, *supra* note 330, at 641. It has been argued, however, that evidence obtained through a *jus cogens* violation—for instance, torture—should be deemed inadmissible. Wolfrum, *supra* note 36, at 563.

337. *U.K. v. Alb.*, 1949 I.C.J. at 18.

338. United States Diplomatic and Consular Staff in Tehran (U.S. v. Iran), 1980 I.C.J. 64, para. 13 (May 24).

-Even if a litigant obtains evidence illegally, e.g., through an unauthorized intrusion into the computer systems of another State, the evidence so obtained may be taken into account by the Court, although the purpose of collecting evidence does not exclude the illegality of the conduct.

Cyber Sovereignty: The Way Ahead

ERIC TALBOT JENSEN*

SUMMARY

---

* Associate Professor, Brigham Young University Law School. The author would like to thank the staff of the *Texas International Law Journal* for hosting an excellent symposium and the attendees for their insights and comments to the author's presentation. Additionally, Grant Hodgson and Brooke Robinson provided excellent research and review assistance for this Article.

PREFACE

> There is no universally agreed definition [for sovereignty], but considerations of international sovereignty revolve around the recognition of a government's right to exercise exclusive control over territory, and this definition is ill suited for cyber discussions. For convenience we might refer to "the geography of cyberspace," but I challenge you to point to cyberspace. Although cyberspace is all around us, when trying to point at it you will be as unable to as the Square in [Edwin] Abbott's Flatland was to point to "up." I always found it troubling to hear military commanders talk in terms of seizing the cyber "high ground" or negotiating "cyber terrain." That was language they were comfortable with, but in any meaningful sense of the word, cyber lacks geography.[1]

Recent years are full of reports of cyber incidents in which, from time to time, significant damage is done by way of a cyber operation. Examples include the 2007 cyber assault on Estonia by pro-Russian "hacktivists" that temporarily shut down many governmental and private sector operations,[2] the 2012 "Shamoon" virus that damaged 30,000 computers at Saudi Arabia's Aramco and was claimed by the "Cutting Sword of Justice,"[3] the 2013 cyber shutdown of the New York Times by the Syrian Electronic Army,[4] and of course the infamous Stuxnet malware that damaged almost one thousand centrifuges at an Iranian nuclear facility and has been attributed to the United States and Israel by many cyber experts.[5]

---

1. Gary D. Brown, *The Wrong Questions About Cyberspace*, 217 MIL. L. REV. 214, 225–26 (2013). Gary Brown was the first Staff Judge Advocate (legal advisor) for the newly formed United States Cyber Command. *Id.* at 214.

2. Kertu Ruus, *Cyber War I: Estonia Attacked from Russia*, EUR. INST. (2008), http://www.europeaninstitute.org/index.php/component/content/article/42-european-affairs/winterspring-2008/67-cyber-war-i-estonia-attacked-from-russia (discussing the cyber attacks on Estonia and Estonia's defensive response).

3. *Saudi Arabia Says Cyber Attack Aimed to Disrupt Oil, Gas Flow*, REUTERS (Dec. 9, 2012, 2:30 PM), http://www.reuters.com/article/2012/12/09/saudi-attack-idUSL5E8N91UE20121209; *see also* Wael Mahdi, *Saudi Arabia Says Aramco Cyberattack Came from Foreign States*, BLOOMBERG (Dec. 9, 2012), http://www.bloomberg.com/news/2012-12-09/saudi-arabia-says-aramco-cyberattack-came-from-foreign-states.html.

4. Heather Kelly, *Syrian Group Cited as* New York Times *Outage Continues*, CNN (Aug. 29, 2013, 9:30 AM), http://www.cnn.com/2013/08/27/tech/web/new-york-times-website-attack/ (discussing the attack that temporarily shut down the *New York Times*' website).

5. Ellen Nakashima & Joby Warrick, *Stuxnet Was Work of U.S. and Israeli Experts, Officials Say*, WASH. POST, June 2, 2012, http://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html.

Each of these cyber events, and the multitude of others that have occurred and continue to occur daily,[6] raises important questions about the role and responsibility of States with respect to cyber incidents. Do States exercise sovereign control over the cyber infrastructure that sits on their territory? If so, do States have a responsibility to control the cyber activities that emanate from or even just pass through their sovereign cyber assets? In other words, to what extent does a State have to control activities of non-State actors, such as private hacktivists, criminal organizations, and terrorists, when those cyber actions may cause harm to others?

The answer to these questions revolves in large part around the international law doctrine of sovereignty.[7] The extent to which nations exercise sovereignty over cyberspace and cyber infrastructure will provide key answers to how much control States must exercise and how much responsibility States must accept for harmful cyber activities when they fail to adequately do so.

This Article argues that States have sovereign power over their cyber infrastructure and that with that sovereign power comes corresponding responsibility to control that infrastructure and prevent it from being knowingly used to harm other States. This responsibility to prevent external harm extends not

---

6. *See generally* A FIERCE DOMAIN: CONFLICT IN CYBERSPACE, 1986 TO 2012 (Jason Healey ed., 2013).

7. The continuing application of international law to cyber capabilities has led one scholar to conclude:

> This does not necessarily mean that the rules and principles of international law are applicable to cyberspace in their traditional interpretation. Because of the novel character of cyberspace, and in view of the vulnerability of cyber infrastructure, there is a noticeable uncertainty among governments and legal scholars as to whether the traditional rules and principles are sufficient to provide answers to some worrisome questions.

Wolff Heintschel von Heinegg, *Territorial Sovereignty and Neutrality in Cyberspace*, 89 INT'L L. STUD. 123, 127 (2013). China, Russia, Tajikistan, and Uzbekistan seem to believe that new treaties governing cyber conflict are needed. *See* Permanent Representatives of China, the Russian Federation, Tajikistan, and Uzbekistan to the United Nations, Letter dated 12 Sept. 2011 to the Secretary-General, U.N. Doc. A/66/359 (Sept. 14, 2011) ("China, Russia, Tajikistan and Uzbekistan have jointly elaborated in the form of a potential General Assembly resolution on an international code of conduct for information security and call for international deliberations within the United Nations framework on such an international code, with the aim of achieving the earliest possible consensus on international norms and rules guiding the behaviour of States in the information space." (citation omitted)); Wu Jiao & Zhao Shengnan, *Nations Call on UN to Discuss Cyber Security*, CHINA DAILY, Sept. 14, 2011, http://europe.chinadaily.com.cn/europe/2011-09/14/content_13682694.htm (discussing letter from China, Russia, Tajikistan, and Uzbekistan to United Nations calling for new rules for cyber conflict); Jason Healey, *Breakthrough or Just Broken? China and Russia's UNGA Proposal on Cyber Norms*, ATLANTIC COUNCIL (Sept. 21, 2011), http://www.atlanticcouncil.org/blogs/new-atlanticist/breakthrough-or-just-broken-china-and-russia-s-unga-proposal-on-cyber-norms [hereinafter Healey, *Breakthrough or Just Broken?*] (same). However, other countries, including the United Kingdom and the United States, have advocated that current international law is insufficient to govern cyber war. *See, e.g.*, U.N. Secretary-General, *Developments in the Field of Information and Telecommunications in the Context of International Security: Rep. of the Secretary-General: Addendum*, at 4, U.N. Doc. A/59/116/Add.1 (Dec. 28, 2004) (discussing the United States' acknowledgment of the need for international cooperation to assure cybersecurity); U.N. Secretary-General, *Developments in the Field of Information and Telecommunications in the Context of International Security: Rep. of the Secretary-General*, at 11–12, U.N. Doc. A/59/116 (June 23, 2004) (asserting the United Kingdom's position that the Council of Europe Convention on Cybercrime is the best means for criminalizing cybercrime).

only to State actors, but also to non-State actors. This sovereign power and responsibility, while almost exclusive, necessarily has some limitation.

The Introduction to this Article will introduce the underlying assumptions of sovereignty and set the stage for a review of some of the cardinal principles of sovereignty and their application to cyberspace in light of each State's corresponding sovereign duties and obligations. Parts I and II will then look at the fundamental principles of sovereignty, consider how these principles apply to cyber activities and what corresponding cyber duties and obligations those principles implicate, and then consider related issues that naturally arise from that application.

INTRODUCTION

In the emerging area of cyber operations, the application of the doctrine of sovereignty to cyber activities has created an ongoing debate among States,[8] academics,[9] and practitioners.[10] The recently published *Tallinn Manual on the International Law Applicable to Cyber Warfare* (*Tallinn Manual*) reflects some of this controversy in its short section on sovereignty.[11]

Current State practice suggests that States are hesitant to accept responsibility for cyber activities that come from within their sovereign territory.[12] In none of the examples discussed in the Preface did any State accept responsibility for the cyber actions that occurred.[13] In fact, the opposite is true. In the case of the cyber assaults on Estonia, Russia not only disclaimed any responsibility, but has proven unresponsive to requests by Estonia for investigation and extradition of the potential offenders who acted from within Russian territory.[14] In the case of the

8. *See generally* Grp. of Governmental Experts on Devs. in the Field of Info. and Telecomms. in the Context of Int'l Sec., *Rep. of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (2010), *transmitted by Note of the Secretary-General*, U.N. Doc. A/65/201 (July 30, 2010) [hereinafter Int'l Sec. Grp.] (chronicling States' approaches to cybersecurity); U.N. Secretary-General, *Developments in the Field of Information and Telecommunications in the Context of International Security: Rep. of the Secretary-General*, U.N. Doc. A/64/129/Add.1 (Sept. 9, 2009) [hereinafter *Developments in the Field of Information and Telecommunications*] (reporting on how States have responded to the security concerns surrounding new developments in the fields of information and telecommunications).

9. *See, e.g.*, *generally* Forrest Hare, *Borders in Cyberspace: Can Sovereignty Adapt to the Challenges of Cyber Security?*, *in* THE VIRTUAL BATTLEFIELD: PERSPECTIVES ON CYBER WARFARE 88 (Christian Czosseck & Kenneth Geers eds., 2009); Andrew Liaropoulos, *Exercising State Sovereignty in Cyberspace: An International Cyber-Order under Construction?*, *in* PROCEEDINGS OF THE 8TH INTERNATIONAL CONFERENCE ON INFORMATION WARFARE AND SECURITY 136 (Douglas Hart ed., 2013); von Heinegg, *supra* note 7; Sean Kanuck, *Sovereign Discourse on Cyber Conflict under International Law*, 88 TEX. L. REV. 1571, 1597 (2010); Eric Talbot Jensen, *Sovereignty and Neutrality in Cyber Conflict*, 35 FORDHAM INT'L L.J. 815 (2012) [hereinafter Jensen, *Sovereignty and Neutrality*].

10. Brown, *supra* note 1, at 218.

11. TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE r. 1 (Michael N. Schmitt ed., 2013) [hereinafter TALLINN MANUAL]. The Author was a member of the international group of experts that drafted the Manual.

12. *See* Michael N. Schmitt, *The Law of Cyber Warfare:* Quo Vadis?, 25 STAN. L. & POL'Y REV. 269, 277 (2014) [hereinafter Schmitt, *The Law of Cyber Warfare*] ("[I]t is typically left to potential targeted states to safeguard cyber activities and cyber infrastructure on their territory.").

13. *See supra* notes 2–5 and accompanying text.

14. *See* Ruus, *supra* note 2 (discussing lack of Russian cooperation following the attack).

Stuxnet malware, despite numerous allegations that the United States and Israel were involved, neither country has officially admitted responsibility.[15]

This hesitation on the part of States to accept responsibility for incidents that occur over the Internet is the product of two major issues inherent in the structure of the Internet: the difficulty of timely attributing an attack and the random method in which data travels over the Internet infrastructure, normally taking the path of least resistance without respect to geography.[16]

The issue of cyber attribution has been well documented[17] and needs only brief comment here. The nature of the Internet allows anonymity, including for those who desire to represent themselves to be someone else. This anonymity acts as "an open invitation to those who would like to do [] harm, whatever their motives."[18] This inherent difficulty in timely attribution makes States wary of accepting responsibility for attacks from within their territory because not only can they not always identify the attacker in a timely manner, but because even if they can identify the computer from which the cyber act originates, they are unlikely to know who is behind the computer.[19]

Similarly, anonymity allows States to take actions, knowing that timely attribution is impossible.[20] This is especially true of actions taken by States through proxies, such as non-State actors.[21]

---

15. David E. Sanger, *Obama Order Sped up Wave of Cyberattacks against Iran*, N.Y. TIMES, June 1, 2012, http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=2&_r=2&seid=auto&smid=tw-nytimespolitics&pagewanted=all&; *but see* William J. Broad et al., *Israeli Test on Worm Called Crucial in Iran Nuclear Delay*, N.Y. TIMES, Jan. 15, 2011, http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?pagewanted=all (noting tacit U.S. and Israeli acknowledgment of the Stuxnet virus).

16. *See* David Hricik, *Lawyers Worry Too Much about Transmitting Client Confidences by Internet E-mail*, 11 GEO. J. LEGAL ETHICS 459, 466–70 (1998) (outlining the complex process through which information is fragmented and disseminated through the internet according to the best path available, creating a random set of transmission paths at any moment).

17. *See generally* MARTIN C. LIBICKI, CYBERDETERRENCE AND CYBERWAR (2009); Jack M. Beard, *Legal Phantoms in Cyberspace: The Problematic Status of Information as a Weapon and a Target under International Humanitarian Law*, 47 VAND. J. TRANSNAT'L L. 67 (2014); Susan W. Brenner, *Cyber-Threats and the Limits of Bureaucratic Control*, 14 MINN. J. L. SCI. & TECH. 137 (2013); Duncan B. Hollis, *An e-SOS for Cyberspace*, 52 HARV. INT'L L.J. 373, 397–401 (2011); Todd C. Huntley, *Controlling the Use of Force in Cyber Space: The Application of the Law of Armed Conflict during a Time of Fundamental Change in the Nature of Warfare*, 60 NAVAL L. REV. 1, 34–35 (2010); Erik M. Mudrinich, *Cyber 3.0: The Department of Defense Strategy for Operating in Cyberspace and the Attribution Problem*, 68 A.F. L. REV. 167 (2012); Bradley Raboin, *Corresponding Evolution: International Law and the Emergence of Cyber Warfare*, 31 J. NAT'L ASS'N ADMIN. L. JUDICIARY 602 (2011); Michael N. Schmitt, *"Below the Threshold" Cyber Operations: The Countermeasures Response Option and International Law*, 54 VA. J. INT'L L. 697 (2014); Jonathan Solomon, *Cyberdeterrence between Nation-States: Plausible Strategy or a Pipe Dream?*, 5 STRATEGIC STUD. Q. 1, 5–10 (2011), *available at* http://www.au.af.mil/au/ssq/2011/spring/solomon.pdf.

18. Harry D. Raduege, Jr., *Fighting Weapons of Mass Disruption: Why America Needs a "Cyber Triad"*, *in* GLOBAL CYBER DETERRENCE: VIEWS FROM CHINA, THE U.S., RUSSIA, INDIA, AND NORWAY 3, 4 (Andrew Nagorski ed., 2010), *available at* http://www.ewi.info/sites/default/files/ideas-files/CyberDeterrenceWeb.pdf.

19. Eric Talbot Jensen, *Cyber Deterrence*, 26 EMORY INT'L L. REV. 773, 785–86 (2012).

20. *See id.* (discussing how the difficulty of attributing cyber attacks enables cyber attackers).

21. *See id.* at 781 (emphasizing the ability of non-State actors to carry out attacks and "harness the

Additionally, the nature of data flow on the Internet makes States hesitant to accept responsibility for cyber activities that flow from within their territory. Cyber data, by its nature, seeks out the path of least resistance over the available cyber infrastructure.[22] In other words, an email sent from a computer in one city to a recipient in that same city may travel through any number of foreign countries before arriving at its destination.[23] The same is true of cyber malware. And this data is not only uncontrollable by the sender in how it travels, but also largely uncontrollable by the States through which the data passes. This means that malware may traverse any number of States before reaching the target State. Transit States do not want to be responsible for the harmful data in these types of scenarios.

Despite the hesitance of States to accept responsibility for attacks crossing their cyber infrastructure, there is a fundamental assumption in international law that authority and obligations strive to stay in balance with each other.[24] In other words, when the international paradigm allocates authority to a State, it almost always allocates a corresponding responsibility or obligation.[25] The application of this principle was illustrated as far back in history as the legitimization of the Westphalian system. When States became the primary actors in the international community, they did so with the understanding that they would possess a monopoly on force within their geographic borders.[26] In correspondence to that obligation came the grant of authority for sovereigns to raise armies and navies that would be reciprocally recognized by other States and given combatant immunity in any future conflicts, as long as those armies and navies acted in accordance with the sovereign's wishes and the provisions of any international agreements to which the sovereign had acceded.[27]

The practical application of this balance is seen in the Instruction for the Government of Armies of the United States in the Field,[28] known as the Lieber

---

power of cyber weapons and use them at their discretion" without the threat of retribution).

22. *See* Hricik, *supra* note 16, at 467 (noting that the internet "is based on TCP/IP (Transfer Control Protocol/Internet Protocol) routing of information packets through unpredictable paths through interconnected networks linking millions of computers." (internal quotation marks omitted)).

23. *See id.* at 469 (explaining how an email can "be broken into hundreds or thousands of packets, each potentially traversing several different networks around the globe" before reaching its destination (internal quotation marks omitted)).

24. *See* Martti Koskenniemi, *Doctrines of State Responsibility*, *in* THE LAW OF INTERNATIONAL RESPONSIBILITY 45, 47–48 (Philip Alston & Vaughan Lowe eds., 2010) (discussing the reciprocal nature of authority and obligations in international law).

25. *Id.*

26. W. Michael Reisman, *Sovereignty and Human Rights in Contemporary International Law*, 84 AM. J. INT'L L. 866, 867 (1990); Frédéric Gilles Sourgens, *Positivism, Humanism, and Hegemony: Sovereignty and Security for Our Time*, 25 PENN ST. INT'L L. REV. 433, 443 (2006) (citing sixteenth-century writer Bodin's *Six Livres De la République* as defining sovereignty as the "absolute and perpetual power of the commonwealth resting in the hands of the state"). *See generally* PHILIP BOBBITT, THE SHIELD OF ACHILLES: WAR, PEACE, AND THE COURSE OF HISTORY 81–90, 96–118 (2002) (discussing the development of the concept of sovereign power).

27. *See* Viet D. Dinh, *Nationalism in the Age of Terror*, 56 FLA. L. REV. 867, 871–73 (2004) (discussing key characteristics of the Westphalian system, including the State monopoly on violence); *cf.* BOBBITT, *supra* note 26, at 509–19 (recounting the development of the Westphalian system and Grotius's ideas of sovereignty).

28. U.S. War Department, General Orders No. 100: Instructions for the Government of Armies of the United States in the Field (Apr. 24, 1863) [hereinafter Lieber Code], *available at* http://www.icrc.org

Code.[29] This Code was written by Francis Lieber and issued by President Abraham Lincoln to provide guidance to the Union armies during the American Civil War.[30] Article 57 of the Lieber Code proclaims, "So soon as a man is armed by a sovereign government and takes the soldier's oath of fidelity, he is a belligerent; his killing, wounding, or other warlike acts are not individual crimes or offenses."[31] In other words, once the sovereign was exercising the responsibility to monopolize and control violence through its agents, those agents were granted authority to use force on behalf of the sovereign with immunity, even when fighting against other sovereigns.[32]

This balance between responsibility and authority continues to underlie the modern law of armed conflict. The laws with respect to prisoners of war,[33] the treatment of civilians during armed conflict,[34] and targeting[35] all reflect the balanced grant of authority and obligation. The balance also applies directly to the principle of sovereignty. As stated in the International Court of Justice's (ICJ) *Corfu Channel* case, "Sovereignty confers rights upon States and imposes obligations on them."[36]

As a starting point, it is important to note that international law must also be considered to apply to cyberspace and cyber technologies. As stated in the United States' 2011 International Strategy for Cyberspace, "The development of norms for State conduct in cyberspace does not require a reinvention of customary international law, nor does it render existing international norms obsolete. Long-standing international norms guiding State behavior—in times of peace and conflict—also apply in cyberspace."[37]

/ihl.nsf/FULL/110?OpenDocument.

29. *Id.*; *see also* JOHN FABIAN WITT, LINCOLN'S CODE: THE LAWS OF WAR IN AMERICAN HISTORY 8 (2012) ("Historians and international lawyers who discuss [Instruction for the Government of Armies of the United States in the Field] usually call the order Lieber's code after its principal drafter.").

30. WITT, *supra* note 29, at 2 ("President Lincoln will issue Lieber's code as an order for the armies of the Union. He will deliver it to the armies of the Confederacy, too, and expect them to follow the rules he has set out. The code will be published in newspapers across the country and distributed to thousands of officers in the Union Army.").

31. Lieber Code, *supra* note 28, art. 57.

32. Eric Talbot Jensen, *Applying a Sovereign Agency Theory of the Law of Armed Conflict*, 12 CHI. J. INT'L L. 685, 708–10 (2012).

33. Geneva Convention Relative to the Treatment of Prisoners of War, *opened for signature* Aug. 12, 1949, 6 U.S.T. 3316, 75 U.N.T.S. 135 [hereinafter Geneva Convention on Prisoners of War]; Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I), June 8, 1977, 1125 U.N.T.S. 3 [hereinafter Additional Protocol I].

34. *E.g.*, Geneva Convention Relative to the Protection of Civilian Persons in Time of War, Aug. 12, 1949, 6 U.S.T. 3516, 75 U.N.T.S. 287; Additional Protocol I, *supra* note 33.

35. Additional Protocol I, *supra* note 33.

36. Corfu Channel (U.K. v. Alb.), 1949 I.C.J. 4, 43 (Apr. 9) (individual opinion of Judge Alvarez).

37. EXEC. OFFICE OF THE PRESIDENT OF THE U.S., INTERNATIONAL STRATEGY FOR CYBERSPACE: PROSPERITY, SECURITY, AND OPENNESS IN A NETWORKED WORLD 9 (2011) [hereinafter OFFICE OF THE PRESIDENT, INTERNATIONAL STRATEGY FOR CYBERSPACE], *available at* http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

It follows, then, that the international law doctrines applying to sovereignty would apply to cyber technologies. Where international law grants authority for States with respect to cyberspace and the application of cyber technologies, it also imposes duties and obligations. As nations exercise sovereign power over aspects of cyberspace, or exert sovereign authority over cyber infrastructure, they must necessarily accept the corresponding obligations and duties that come with that assertion of authority.

The following Parts of this Article will review some of the cardinal principles of sovereignty and their application to cyberspace and then consider the corresponding duties and obligations. In each case, the principle of sovereignty will be stated and defined. Its application to cyberspace will then be discussed, including the corresponding duty or obligation that arises from that assertion of sovereignty. An example of the duty and obligation will be used to help clarify the analysis. Finally, issues that arise from the assertion of that authority and its corresponding duty or obligation will be highlighted.

I. STATES ARE SOVEREIGN AND EQUAL

When the nation-State emerged in seventeenth-century Europe, it brought with it the doctrine that the international community would consist of geographically organized and controlled entities that would have at least two characteristics. First, those entities would be sovereign, and second, they would be equal, regardless of size or composition.[38] These two characteristics of States remain in force today and have significant impacts on cyberspace and cyber operations.

A. Sovereignty

Sovereignty is inherent to statehood and, in fact, is often termed the "basic constitutional doctrine of the law of nations."[39] The meaning of the term "sovereignty" has been a point of discussion for centuries[40] and remains so today.[41] However, it is manifested in certain rights and corresponding obligations. A basic review of those rights and obligations will assist in discerning the impact of sovereignty on cyber operations.

---

38. *See* BOBBITT, *supra* note 26, at 508 (noting that in the aftermath of the Thirty Years War, "[t]he extension of the maxim *cuius regio eius religio* imposed common restrictions on states, adumbrating the emergence of a new society of states characterized by their sovereign equality").

39. *E.g.*, JAMES CRAWFORD, BROWNLIE'S PRINCIPLES OF PUBLIC INTERNATIONAL LAW 447 (8th ed. 2012).

40. *E.g.*, SAINT AUGUSTINE, THE CITY OF GOD 88 (Vernon J. Bourke ed., Gerald G. Walsh et al. trans., 1958) (426); JOHN AUSTIN, THE PROVINCE OF JURISPRUDENCE DETERMINED 191–361 (Isaiah Berlin et al. eds., 1954) (1861); THOMAS HOBBES, LEVIATHAN OR THE MATTER, FORME, AND POWER OF A COMMON-WEALTH ECCLESIASTICAL AND CIVILL 121–29 (Richard Tuck ed., 1991) (1651); JOHN LOCKE, TWO TREATISES OF GOVERNMENT 105 (Thomas I. Cook ed., 1947) (1690).

41. *E.g.*, John Alan Cohan, *Sovereignty in a Postsovereign World*, 18 FLA. J. INT'L L. 907, 908–09 (2006); Reisman, *supra* note 26, at 866.

1. Rights

Sovereignty confers rights on two distinct planes or spheres: the domestic sphere and the international sphere. In other words, sovereignty is understood to be "the collection of rights held by a State, first in its capacity as the entity entitled to exercise control over its territory and second in its capacity to act on the international plane, representing that territory and its people."[42]

With respect to the domestic sphere, sovereignty provides exclusivity in power and authority. This was confirmed in the *Island of Palmas* Arbitral Award of 1928.[43] The arbitral decision provides that "[s]overeignty in the relations between States signifies independence. Independence in regard to a portion of the globe is the right to exercise therein, to the exclusion of any other State, the functions of a State."[44] One of the most fundamental rights of sovereignty, then, is exclusivity of power within the sovereign's own territory, particularly as opposed to the exercise of rights in that territory by some other sovereign.[45]

The ICJ in its *Corfu Channel* decision confirmed this understanding of sovereignty. "By sovereingty [sic], we understand the whole body of rights and attributes which a State possesses in its territory, to the exclusion of all other States, and also in its relations with other States."[46]

Though a State's sovereign power is nearly absolute, it is limited by certain international law principles,[47] including actions of the U.N. Security Council,[48] the law of armed conflict,[49] and fundamental human rights.[50] There are also areas where, based on consensual agreement and custom, no State can assert sovereignty, such as the high seas.[51] This area has been treated as *res communis*, meaning that it

---

42. CRAWFORD, *supra* note 39, at 448.

43. Island of Palmas (Neth. v. U.S.), 2 R.I.A.A. 829, 838 (Perm. Ct. Arb. 1928).

44. *Id.*

45. Samantha Besson, *Sovereignty*, *in* MAX PLANCK ENCYCLOPEDIA OF PUBLIC INTERNATIONAL LAW para. 119 (2011). Sovereignty is generally characterized as the "powers and privileges resting on customary law which are independent of the particular consent of another state." CRAWFORD, *supra* note 39, at 448.

46. Corfu Channel (U.K. v. Alb.), 1949 I.C.J. 4, 43 (Apr. 9) (individual opinion of Judge Alvarez).

47. Besson, *supra* note 45, para. 75.

48. For example, each member of the United Nations has agreed to "accept and carry out the decisions of the Security Council in accordance with the present Charter." U.N. Charter art. 25.; *see also* John R. Worth, *Globalization and the Myth of Absolute National Sovereignty: Reconsidering the "Un-signing" of the Rome Statute and the Legacy of Senator Bricker*, 79 IND. L.J. 245, 260 (2004) (discussing States' relinquishment of some powers in accepting the legitimacy and authority of the United Nations).

49. For example, during times of international armed conflicts, States have to treat prisoners of war in accordance with the Geneva Conventions, rather than any potentially applicable domestic law. *See generally* Geneva Convention on Prisoners of War, *supra* note 33.

50. *See* Rosa Ehrenreich Brooks, *War Everywhere: Rights, National Security Law, and the Law of Armed Conflict in the Age of Terror*, 153 U. PA. L. REV. 675, 684–85 (2004) (outlining that "core rights . . . cannot be eliminated"); Ashley S. Deeks, *Consent to the Use of Force and International Law Supremacy*, 54 HARV. INT'L L.J. 1, 11 (2013) (noting that international human rights laws "trump inconsistent domestic laws").

51. Allison Leigh Richmond, *Scrutinizing the Shipwreck Salvage Standard: Should a Salvor Be Rewarded for Locating Historic Treasure?*, 23 N.Y. INT'L L. REV. 109, 121 (2010).

belongs to all States and can be appropriated by no State.[52] There are other areas where actors have agreed to non-exclusive sovereignty such as Antarctica,[53] the seabed,[54] and the moon.[55] These are areas where no sovereign exercises power, but where all sovereigns share power, based on agreement.

2. Obligations

As discussed above, international law tries to keep in balance rights and obligations. This is reflected in the ICJ's statement, "Sovereignty confers rights upon States and imposes obligations on them."[56] Therefore, in correspondence with the rights and authorities discussed above, the principle of sovereignty also imposes obligations which deserve discussion here.

Obligations tied to sovereignty include the obligation to recognize the sovereignty of other States,[57] the obligation of non-intervention into the areas of exclusive jurisdiction of another State,[58] and the obligation to control the actions that occur within the sovereign's geographic boundaries.[59]

The obligation to recognize the sovereignty of other States is simply the obverse of the right of a State to exercise its own sovereignty. In claiming the rights that come with sovereignty, there is an implicit recognition of the right of others to make similar claims and exercise similar rights.

Once another State has made such claims, and those claims are recognized, other sovereigns have a legal obligation to not interfere with the sovereign rights of the other State. Though there are legitimate exceptions to this rule,[60] the obligation of non-intervention is well recognized in international law.[61]

---

52. Jean Allain, *Maritime Wrecks: Where the* Lex Ferenda *of Underwater Cultural Heritage Collides with the* Lex Lata *of the Law of the Sea Convention*, 38 VA. J. INT'L L. 747, 758 (1998).

53. *See* The Antarctic Treaty art. 4, Dec. 1, 1959, 12 U.S.T. 794, 402 U.N.T.S. 71 (limiting claims to sovereignty in Antarctica).

54. U.N. Convention on the Law of the Sea arts. 1, 137, *opened for signature* Dec. 10, 1982, 1833 U.N.T.S. 397.

55. Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies art 2, *opened for signature* Jan. 27, 1967, 18 U.S.T. 2410, 610 U.N.T.S. 205 [hereinafter Outer Space Treaty].

56. Corfu Channel (U.K. v. Alb.), 1949 I.C.J. 4, 43 (Apr. 9) (individual opinion of Judge Alvarez).

57. IAN BROWNLIE, PRINCIPLES OF PUBLIC INTERNATIONAL LAW 289 (7th ed. 2008) ("The sovereignty and equality of states represent the basic constitutional doctrine of the law of nations...."); Michael J. Kelly, *Pulling at the Threads of Westphalia: "Involuntary Sovereignty Waiver"—Revolutionary International Legal Theory or Return to Rule by the Great Powers?*; 10 UCLA J. INT'L L. & FOREIGN AFF. 361, 364 (2005) ("Under classic Westphalian theory, the base maxim upon which foreign relations are built is the proposition that all states are equal and must reciprocally respect each other's sovereignty.").

58. CRAWFORD, *supra* note 39, at 447 ("The corollaries of the sovereignty and equality of states [include] . . . a duty of non-intervention in the area of exclusive jurisdiction of other states . . . .").

59. Ilaşcu v. Moldova, 2004-VII Eur. Ct. H.R. 1, para. 312 ("[J]urisdiction is presumed to be exercised normally throughout the State's territory.").

60. For example, lawful countermeasures or actions taken in self-defense would allow a nation to interfere with another State's sovereignty. *See* U.N. Charter art. 51 (allowing a right of individual or collective self-defense in the event of an armed attack against a Member State of the United Nations).

61. *E.g.*, *Corfu Channel*, 1949 I.C.J. at 35 ("Between independent States, respect for territorial sovereignty is an essential foundation of international relations.").

Another obligation that grows out of sovereignty is the requirement to control actions from within a State's sovereign control from having deleterious effects on others.[62] This obligation is worth mentioning here but will be discussed further below.

B. Equality

The principle of the sovereign equality of States laid out in Article 2.1 of the U.N. Charter States: "The Organization is based on the principle of the sovereign equality of all its Members."[63] This principle of equality is based on the historical maxim "*par in parem non habet imperium*," or "an equal has no power over an equal,"[64] which is considered by some to be the first, and perhaps most fundamental, principle of sovereignty.[65] As such, certain rights and obligations accrue from this accepted equality.

1. Rights

As equals under international law, States have the right to deal with each other on equal footing, with equal consideration under the law. "If states (and only states) are conceived of as sovereign, then in this respect at least they are equal, and their sovereignty is in a major aspect a relation to other states (and to organizations of states) defined by law."[66] While skeptics argue that the practical reality of this is far from being true, with large and powerful States clearly exerting unequal pressures on smaller and weaker States to bow to their desires,[67] equality is still guaranteed under the law. Regardless of what some identify as the reality of international politics where "while all States are equal, some are more equal than others,"[68] the legal regime is established with a clear preference to equality and maintenance of the status quo. "The United Nations are [sic] based on the principle of sovereign equality of all its members and preserving state sovereignty is a top priority for both international organizations and individual States."[69]

---

62. *See infra* Part I.B.2.

63. U.N. Charter art. 2, para. 1.

64. CRAWFORD, *supra* note 39, at 448 & n.9.

65. U.N. Charter art. 2, para. 1.

66. CRAWFORD, *supra* note 39, at 447.

67. *See, e.g.*, *Philippines Seeks Quick UN Ruling on South China Sea Dispute*, S. CHINA MORNING POST, June 19, 2014, http://www.scmp.com/news/asia/article/1536058/philippines-seeks-quick-un-ruling-south-china-sea-dispute ("China claims most of the South China Sea, including waters near the shores of its neighbours, which has led to escalating territorial disputes."); Russell Hotten & Alix Kroeger, *Ukraine-Russia Gas Row: Red Bills and Red Rags*, BBC (June 16, 2014), http://www.bbc.com/news/world-europe-26987082 (stating that the gas conflict is a "power struggle between the interim Ukrainian government, which leans towards the EU, and Russia, which wants to keep Ukraine firmly within its sphere of influence").

68. CRAWFORD, *supra* note 39, at 449 (citing GEORGE ORWELL, ANIMAL FARM 90 (1945)).

69. Liaropoulos, *supra* note 9, at 137–38 (citation omitted).

Some of the obvious rights that accrue from international equality include an equal right to global commons,[70] the right to develop and utilize domestic resources without non-consensual external constraints,[71] and the right to discourse on the international scene as an equal. These rights are also tempered with corresponding obligations.

2. Obligations

Several obligations flow from the principle of sovereign equality. First, States must act with due regard for the rights of other sovereigns.[72] There is some discussion as to how far-reaching this obligation of due regard is, but it is at least applicable by treaty to the global commons,[73] natural resources,[74] the environment,[75] and during times of armed conflict.[76]

The obligation of due regard, though not clearly defined in international law, is generally thought of as an obligation to ensure that the exercise of one State's rights does not cause undue harm to another State's exercise of its rights.[77] It is

---

70. *See* Todd B. Adams, *Is There a Legal Future for Sustainable Development in Global Warming? Justice, Economics, and Protecting the Environment*, 16 GEO. INT'L ENVTL. L. REV. 77, 97 (2003) ("[The world] is to be shared by all generations in accordance with the limited rights and necessary obligations of a user of the natural resources or the trustee of the natural resources .... '[P]lanetary rights' are group rights to equal access to the commons." citing EDITH BROWN WEISS, IN FAIRNESS TO FUTURE GENERATIONS: INTERNATIONAL LAW, COMMON PATRIMONY, AND INTERGENERATIONAL EQUITY 96 (1989))).

71. *See* Inaamul Haque & Ruxandra Burdescu, *Monterrey Consensus on Financing for Development: Response Sought from International Economic Law*, 27 B.C. INT'L & COMP. L. REV. 219, 249–50 (2004) ("Under customary international law, principles of sovereignty support a state's clear right to regulate commercial activities within its borders. This power is extensive and encompasses such issues as capacity to engage in business, forms of business enterprises, conditions of continuance of a business, and regulations of capital markets as well as those of foreign capital inflows and outflows.").

72. *E.g.*, George K. Walker, *Defining Terms in the 1982 Law of the Sea Convention IV: The Last Round of Definitions Proposed by the International Law Association (American Branch) Law of the Sea Committee*, 36 CAL. W. INT'L L.J. 133, 168–69 (2005) ("Article 87(2) declares that the high seas freedoms listed in Article 87(1) ... 'shall be exercised by all States with due regard of the interests of other States in their exercise of the freedom of the high seas, and also with due regard for the rights under [the] Convention with respect to activities in the Area.'" (alteration in original) (quoting U.N. Convention on the Law of the Sea, *supra* note 54, art. 87(2))).

73. *E.g.*, Outer Space Treaty, *supra* note 55, art. 9; Geneva Convention on the High Seas art. 2, Apr. 29, 1958, 13 U.S.T. 2312, 450 U.N.T.S. 82.

74. G.A. Res. 1803 (XVII), U.N. GAOR, 17th Sess., Supp. No. 17, U.N. Doc. A/5217, at 15 (Dec. 14, 1962); Charles N. Brower & John B. Tepe, Jr., *The Charter of Economic Rights and Duties of States: A Reflection or Rejection of International Law?*, 9 INT'L LAW. 295, 306–07 (1975).

75. *See* Meinhard Schröder, *Precautionary Approach/Principle*, *in* MAX PLANCK ENCYCLOPEDIA OF PUBLIC INTERNATIONAL LAW, *supra* note 45, at 4 (describing the precautionary principle as a set of rules guiding States towards environmentally stable development). *See generally* United Nations Conference on Environment and Development, Rio de Janeiro, Braz., June 3–14, 1992, *Report of the United Nations Conference on Environment and Development*, U.N. Doc. A/CONF.151/26/Rev.1 (Vol. I) (Aug. 12, 1992).

76. DEP'T OF THE NAVY ET AL., THE COMMANDER'S HANDBOOK ON THE LAW OF NAVAL OPERATIONS para 8.4 (2007); 1 JEAN-MARIE HENCKAERTS & LOUISE DOSWALD-BECK, CUSTOMARY INTERNATIONAL HUMANITARIAN LAW 147–49 (2005); SAN REMO MANUAL ON INTERNATIONAL LAW APPLICABLE TO ARMED CONFLICTS AT SEA § 35 (Louise Doswald-Beck ed., 1995); U.K. MINISTRY OF DEFENCE, THE MANUAL OF THE LAW OF ARMED CONFLICT para 12.24 (2004).

77. *See* Chinthaka Mendis, Sovereignty vs. Trans-Boundary Environmental Harm: The Evolving

understood to have two components: 1) an "awareness and consideration of either State interest(s) or other factor(s)," and 2) a balancing of those interests and factors when making a decision.[78]

Another obligation that has its foundation in sovereign equality is the obligation to solve disputes peacefully. This obligation is clearly stated in the U.N. Charter[79] and has been stated in General Assembly statements and resolutions,[80] applied in decisions of the ICJ,[81] and has been duplicated in bilateral and multilateral treaties.[82]

While there is no obligation to solve all disputes, States are obligated to resolve disputes peacefully if they have the potential to endanger the maintenance of international peace or security.[83] Additionally, if States elect to resolve disputes that do not endanger international peace and security, they must also resolve these disputes peacefully, though there is no legal obligation to resolve these disputes at all.[84]

C. Application to Cyberspace

As stated above, the doctrine of sovereignty and the principles it espouses have direct application to cyberspace. As States exercise their sovereign rights, they can do so in cyberspace but must also accept the corresponding obligations that apply. The next two Subparts will consider the principles of sovereignty and equality and apply the rights and obligations discussed above to cyberspace, as well as identify some lingering issues that will need further resolution.

1. Sovereignty

As a matter of sovereignty, States have the right to develop their cyber capabilities according to their own desires and resources. A State may choose to extensively develop its cyber capabilities and make them available broadly to its citizens as Estonia has done,[85] or it can choose to close its cyber borders to outside influences as North Korea has done.[86]

International Law Obligations and the Sethusamuduram Ship Channel Project 54–55 (2006) (unpublished U.N. fellowship manuscript), http://www.un.org/depts/los/nippon/unnff_programme_home/fellows_pages/fellows_papers/mendis_0607_sri_lanka.pdf (illustrating the obligation of due regard with discussion of Sri Lanka and India).

78. Walker, *supra* note 72, at 174.

79. U.N. Charter art. 2, paras. 3–4; *Id.* arts. 33–38.

80. G.A. Res. 40/9, U.N. Doc. A/RES/40/9 (Nov. 8, 1985); G.A. Res 2625 (XXV), U.N. GAOR, 25th Sess., U.N. Doc. A/8082, at 121 (Oct. 24, 1970).

81. Aerial Incident of 10 August 1999 (Pak. v. India), Judgment, 2000 I.C.J. 12, para. 53 (June 21).

82. *See id.* para. 22 (noting claims to resolve disputes peacefully in cited bilateral and multilateral treaties).

83. U.N. Charter art. 33, para. 1.

84. G.A. Res. 2625 (XXV), *supra* note 80.

85. *Cyber Security*, E-ESTONIA.COM, http://e-estonia.com/the-story/digital-society/cyber-security/ (last visited Feb. 7, 2015) ("CERT-EE (Computer Emergency Response Team Estonia) handles security

In conjunction with this right, States are obligated to recognize this right and not interfere with the domestic cyber decisions of another State.[87] For example, except as provided by international law, one State cannot place limits on the ability of another with respect to its cyber development and capabilities.[88] States can, either bilaterally or multilaterally, agree to collaborate on cyber activities or place limits or constraints on such development between or among themselves.[89]

Because of the place of a State on the international sphere, States may express their intent and work toward the development of State practice, either alone or in conjunction with others. In line with this, many States have actively participated in international fora, such as the U.N.-sponsored Group of Government Experts,[90] and regional fora, such as the Shanghai Cooperation Organization[91] or the Council of Europe.[92] As with any international agreement, States have the obligation to negotiate in good faith[93] and to comply with their international obligations, once undertaken.

One of the recently developing pressures on the idea of cyber sovereignty is the movement to recognize a human right to the Internet.[94] If the time comes that

---

incidents taking place in the .ee domain. The department helps in case Estonian websites or services should fall under cyber attack or if Estonian computers distribute malware. CERT-EE also has the possibility to reverse engineer the malware .... [T]he real key to Estonian cyber security lies in the inherent safety and security built-in to every single Estonian e-Government and IT infrastructure system. The secure 2048-bit encryption that powers Estonia's Electronic-ID, digital signatures and X-road-enabled systems means that personal identity and data in Estonia is airtight.").

86. Dave Lee, *North Korea: On the Net in World's Most Secretive Nation*, BBC (Dec. 10, 2012), http://www.bbc.com/news/technology-20445632.

87. *See* TALLINN MANUAL r. 1 (observing that sovereignty gives States the exclusive right to control cyber infrastructure and cyber activities within their boundaries).

88. *See id.* (delineating exclusive rights associated with State sovereignty in cyberspace).

89. *See, e.g.*, U.S. DEP'T OF DEF., DEPARTMENT OF DEFENSE STRATEGY FOR OPERATING IN CYBERSPACE 9 (2011) [hereinafter DEPARTMENT OF DEFENSE STRATEGY FOR OPERATING IN CYBERSPACE], *available at* http://www.defense.gov/home/features/2011/0411_cyberstrategy/docs/DOD_Strategy_for_Operating_in_Cyberspace_July_2011.pdf (describing the Department of Defense's plan to develop "increasingly robust international relationships to reflect [its] core commitments and common interests in cyberspace").

90. Int'l Sec. Grp., *supra* note 8, at 7–8.

91. Oona A. Hathaway et al., *The Law of Cyber-Attack*, 100 CALIF. L. REV. 817, 865–66 (2012).

92. Convention on Cybercrime pmbl., Nov. 23, 2001, T.I.A.S No. 13174, E.T.S. No. 185 (2001) [hereinafter Convention on Cybercrime].

93. *See, e.g.*, Aerial Incident of 10 August 1999 (Pak. v. India), Judgment, 2000 I.C.J. 12, para. 53 (June 21) ("The Court's lack of jurisdiction does not relieve States of their obligation to settle their disputes by peaceful means .... They are [ ] under an obligation to seek [a peaceful settlement], and to do so in good faith ...."); G.A. Res. 2625 (XXV), *supra* note 80, at 123 (reaffirming U.N. Charter principles related to peaceful resolution of conflicts); Draft Declaration on Rights and Duties of States, G.A. Res. 375 (IV), annex art. 13, U.N. GAOR, 4th Sess., U.N. Doc. A/1251, at 67 (Dec. 6, 1949) ("Every State has the duty to carry out in good faith its obligations arising from treaties and other sources of international law ...."); Markus Kotzur, *Good Faith (Bona Fide)*, *in* MAX PLANCK ENCYCLOPEDIA OF PUBLIC INTERNATIONAL LAW, *supra* note 45, paras. 11–14 (discussing treaties that require good-faith negotiation).

94. *See* Written Statement Submitted by the Association for Progressive Communications (APC), a Non-Governmental Organization in General Consultative Status, U.N. Doc. A/HRC/17/NGO/38 (May 24, 2011) (associating "Internet rights" with human rights). *See also* Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, *Rep. of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, para. 22, U.N. Doc. A/HRC/17/27 (May 16, 2011) ("The right to freedom of opinion and expression is as much

such a human right is recognized and accepted by States, that right will, of course, impose obligations on the sovereign decisions of each State, constraining State action that might affect the enjoyment of that human right by its population.

Additionally, a State's exercise of sovereignty over cyber resources can be directed or limited by the U.N. Security Council through the power granted to it in the U.N. Charter.[95] States have a duty to comply with Security Council resolutions, even if they limit the exercise of sovereignty over cyber issues. Additionally, States must comply with human rights obligations, even if it limits their exercise of sovereignty.[96]

For example, assume State A contracts for the use of cyber capabilities from State C. Assume further that State A is using cyber means to incite human rights abuses in State B through the cyber infrastructure provided by State C. If the Security Council orders State C to stop allowing State A to use its cyber infrastructure, State C must comply.

2. Equality

Just as States are equals under the doctrine of sovereignty, each State exercises its sovereign cyber prerogatives on an equal plane with all others. Each State, regardless of its cyber capabilities, has the same right to exercise sovereignty over its territory as any other State. However, in doing so, conflicts often arise between States.[97] Certain obligations attach to States in these disputes.

First, States have an obligation to resolve peacefully cyber disputes that may endanger international peace and security.[98] If States attempt to resolve cyber disputes that don't endanger international peace and security, they must do so peacefully.[99]

For example, if State A is using cyber means to harm State B, and that action is endangering international peace and security, both States have an obligation to resolve the dispute peacefully. Alternatively, if State A is using cyber means to steal information from State B, but that theft of information does not endanger

---

a fundamental right on its own accord as it is an 'enabler' of other rights . . . ."); Cassondra Mix, *Internet Communication Blackout: Attack Under Non-international Armed Conflict?*, 3 J.L. & CYBER WARFARE 70, 99 (2014) (noting the suggestions that an Internet blackout imposed by Egyptian authorities to quell protests in 2011 may have violated a right to the Internet).

95. U.N. Charter art. 25 ("The Members of the United Nations agree to accept and carry out the decisions of the Security Council in accordance with the present Charter.").

96. *See, e.g.*, International Covenant on Civil and Political Rights, *opened for signature* Dec. 16, 1966, 999 U.N.T.S. 171 (establishing the civil and political rights of all individuals as well as States' obligations to protect those rights).

97. *See, e.g.*, Lesley Wroughton & Michael Martina, *Cyber Spying, Maritime Disputes Loom Large in U.S.-China Talks*, REUTERS (July 8, 2014), http://www.reuters.com/article/2014/07/08/china-usa-idUSL4N0PJ0MT20140708 (noting increased tensions between the United States and China regarding the territorial scope of cyber activities).

98. *See* U.N. Charter art. 2, para. 3 ("All Members shall settle their international disputes by peaceful means in such a manner that international peace and security, and justice, are not endangered.").

99. *Id.*

international peace and security, a dispute may arise, but there is no obligation to try to settle that dispute. However, if attempts to settle that dispute are made, those methods must be peaceful.

Second, in its cyber activities, a State must exercise due regard for the rights of other States.[100] For example, assume a State wants to increase its cyber security. In an effort to do so, it decides to aggressively monitor cyber threats across the World Wide Web. That State has the right to do so, so long as its activities do not violate the rights of other sovereign States.

D. The Way Ahead

This principle of sovereign equality raises some lingering issues that continue to be the focus of the international community. Because States are sovereign and equal, each State is able to develop its cyber capabilities based on its own best interest. Further, each State has no obligation to get involved in other States' domestic cyber issues unless it chooses to do so. However, there is a great deal of discussion about cyber collaboration, particularly as it relates to less developed countries.

The U.N. Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security recently stated in its report that "[c]onfronting the challenges of the twenty-first century depends on successful cooperation among like-minded partners. Collaboration among States, and between States, the private sector and civil society, is important and measures to improve information security require broad international cooperation to be effective."[101] This collaboration would "be designed to share best practices, manage incidents, build confidence, reduce risk and enhance transparency and stability."[102]

Information sharing and capacity building claims revolve mostly around calls for "ensuring global [information and communications technology] security,"[103] and many States have responded favorably to some of these ideas.[104] In the Department of Defense's Cyberspace Policy Report, the Department of Defense stated,

> In collaboration with other U.S. Government agencies, Allies and partners, [the Department of Defense] pursues bilateral and

100. *See supra* notes 72–78 and accompanying text (discussing the duty of due regard and its broad applicability under international law).

101. Int'l Sec. Grp., *supra* note 8, para. 15.

102. *Id.* para. 14.

103. *E.g.*, *id.* para. 17.

104. *See, e.g.*, *EU–Japan ICT Cooperation–Joining Forces for the Future Internet*, EUR. COMM'N, https://ec.europa.eu/digital-agenda/en/eu-japan-ict-cooperation-%E2%80%93-joining-forces-future-internet (last visited Feb. 8, 2015) (stating that European countries began joint research projects with Japan in 2012 to design efficient, global technology, including internet security technologies, "for the future networked society"); Press Release, White House, FACT SHEET: U.S.-Russian Cooperation on Information and Communications Technology Security (June 17, 2013), *available at* http://www.whitehouse.gov/the-press-office/2013/06/17/fact-sheet-us-russian-cooperation-information-and-communications-technol (indicating that the United States and Russian Federation took measures to increase cooperation on information and communications technology security in order to reduce the possibility of a cyber incident destabilizing their bilateral relationship).

> multilateral engagements to develop further norms that increase openness, interoperability, security, and reliability. International cyberspace norms will increase stability and predictability of state conduct in cyberspace, and these norms will enable international action to take any required corrective measures.[105]

The balance that will have to be struck between the exercise of sovereign prerogative with respect to cyber activities and the benefits of information and security sharing for the health of the Internet will continue to be a vexing issue for the foreseeable future. For now, there is no obligation to engage in information and security sharing, but much pressure to do so.

Finally, the equality of States means that each State has an equal vote in the discussion of how to resolve lingering cyber issues. For example, a group of States headed by Russia recently proposed a "code of conduct" for cyber activities.[106] Other nations, such as the United States, did not support such an initiative.[107] States may choose to band together in regional alliances with respect to cyber activities[108] or may take unilateral action.[109] No consensus is required in a system of sovereign equality.

II. STATES EXERCISE SOVEREIGNTY OVER TERRITORY, PERSONS, AND ACTIVITIES

Though sovereignty manifests itself in many different ways, it almost always means that a sovereign has some kind of territory over which it exercises ultimate control.[110] This territorial authority extends to the population and activities within the territory.[111] As clearly stated in one of the seminal treatises on international law, "The corollaries of the sovereignty and equality of states [include] a jurisdiction, prima facie exclusive, over a territory and the permanent population living there . . . ."[112]

---

105. U.S. DEP'T OF DEF., DEPARTMENT OF DEFENSE CYBERSPACE POLICY REPORT 5-6 (2011) [hereinafter DEPARTMENT OF DEFENSE CYBERSPACE POLICY REPORT] *available at* http://www.defense.gov/home/features/2011/0411_cyberstrategy/docs/NDAA%20Section%20934%20Report_For%20webpage.pdf.

106. Wu & Zhao, *supra* note 7.

107. Healey, *Breakthrough or Just Broken?*, *supra* note 7.

108. *See* JOHN LYONS, ESTABLISHING THE INTERNATIONAL CYBER SECURITY PROTECTION ALLIANCE IN ASIA PACIFIC (ICSPA APAC) 1 (2014) (announcing the establishment of an alliance in the Asia Pacific to enhance online safety and security and provide governments and law enforcement agencies with resources and expertise to help them reduce harm from cyber crime).

109. Abraham D. Sofaer et al., *Cyber Security and International Agreements*, *in* PROCEEDINGS OF A WORKSHOP ON DETERRING CYBERATTACKS: INFORMING STRATEGIES AND DEVELOPING OPTIONS FOR U.S. POLICY 179, 179 (The Nat'l Acad. Press ed., 2010) ("[C]urrent U.S. efforts to deter cyberattacks and exploitation—though formally advocating international cooperation—are based almost exclusively on unilateral measures.").

110. *See* Besson, *supra* note 45, para. 1 (defining sovereignty as "supreme authority within a territory).

111. *Id.* para. 70 (referring to sovereignty as encompassing "ultimate authority and competence over all people and all things within [the sovereign's] territory").

112. CRAWFORD, *supra* note 39, at 447.

The rest of Part II will discuss the sovereign rights and obligations with respect to territory and persons, and then apply these rights and obligations to cyberspace, including identifying particular issues that remain unsettled.

A. Territory

Sovereignty over a territory denotes certain rights and corresponding obligations associated with that specific territory.

1. Rights

Perhaps the most important sovereign right over territory is the exclusivity of authority. As von Heinegg has stated, "territorial sovereignty protects a State against any form of interference by other States."[113] Sovereigns alone exercise this right and are only encroached upon through consensual divestiture of authority.[114] Even the UN Charter grants States protection under Article 2(7) against intervention from the United Nations, and other States in certain matters, concerning issues that fall within a State's domestic jurisdiction.[115]

Sovereignty over territory necessarily implies sovereignty over things found on or within territory. For example, "[O]bjects owned by a State or used by that State for exclusively non-commercial government purposes are an integral part of the State's sovereignty and are subject to the exclusive jurisdiction of that State if located outside the territory of another State."[116] This exclusivity of jurisdiction would also apply to objects that have sovereign immunity, wherever located.[117] Additionally, objects not owned by the State but located within the State's territory are subject to the State's regulation.[118] This would include both real and personal property.[119]

States also exercise authority to control their geographic borders.[120] This implies that "the State is entitled to control access to and egress from its territory," which "seems to also apply to all forms of communication."[121]

---

113. von Heinegg, *supra* note 7, at 124.

114. *See* Cohan, *supra* note 41, at 935 (explaining how States can willingly enter into agreements that undermine their domestic sovereignty by recognizing external authority structures).

115. U.N. Charter art. 2, para. 7; Besson, *supra* note 45, para. 88 ("The UN Charter also protects sovereign States' domaine réservé and prohibits other States' intervention on sovereign States' territory." (citations omitted)).

116. von Heinegg, *supra* note 7, at 130.

117. TALLINN MANUAL r. 4.

118. von Heinegg, *supra* note 7, at 124.

119. HENRY WHEATON, ELEMENTS OF INTERNATIONAL LAW § 77 (George Grafton Wilson ed., 1936) (1836).

120. Hare, *supra* note 9, at 92.

121. von Heinegg, *supra* note 7, at 124.

2. Obligations

The principle of sovereign equality entails an obligation of all States to respect the territorial sovereignty of other States. As the ICJ noted in the *Nicaragua* judgment, "[b]etween independent States, respect for territorial sovereignty is an essential foundation of international relations."[122]

Another extremely important obligation that each sovereign State has is to not knowingly allow its territory to be used to harm another State.[123] This obligation is well founded in international law and stated clearly in the ICJ's *Corfu Channel* case where the court says a State may not "allow knowingly its territory to be used for acts contrary to the rights of other States."[124]

Accordingly, States are required under international law to take appropriate steps to protect the rights of other States.[125] This obligation applies not only to criminal acts harmful to other States, but also, for example, to activities that inflict serious damage or have the potential to inflict such damage on persons and objects protected by the territorial sovereignty of the target State.[126]

These obligations, as applied to cyber operations, generate interesting discussion, as will be covered in further detail below. While it is mostly clear how they apply in the non-cyber world, cyber operations have caused many to rethink the practical application of these foundational sovereign obligations.[127]

B. Persons

The ability of a sovereign State to assert power over persons has been uncontroversial since the genesis of statehood.[128] However, the bounds of that

122. Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, para. 202 (June 27) (quoting another source).

123. Corfu Channel (U.K. v Alb.), 1949 I.C.J. 4, 22 (Apr. 9).

124. *Id.*

125. *See, e.g.*, United States Diplomatic and Consular Staff in Tehran (U.S. v. Iran), Judgment, 1980 I.C.J. 3, paras. 67–68 (May 24) (describing the general obligation under international law for States to "ensure the most constant protection and security to each other's nationals in their respective territories." (internal quotation marks omitted)).

126. In the *Trail Smelter* case, the arbitral tribunal, citing the Federal Court of Switzerland, noted: "This right (sovereignty) excludes . . . not only the usurpation and exercise of sovereign rights . . . but also an actual encroachment which might prejudice the natural use of the territory and the free movement of its inhabitants." Trail Smelter (U.S. v. Can.), 3 R.I.A.A. 1905, 1963 (1941) (first omission and part of second omission in original). According to the tribunal, "under the principles of international law . . . no State has the right to use or permit the use of its territory in such a manner as to cause injury by fumes . . . in or to the territory of another or the properties or persons therein, when the case is of serious consequence . . . ." *Id.* at 1965.

127. *See, e.g.*, Eric Talbot Jensen, *State Obligations in Cyber Operations*, 14 BALTIC Y.B. INT'L L. 71 (2014) [hereinafter Jensen, *State Obligations*], *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2419527 (describing how recent cyber incidents have drawn attention to State obligations to control their cyber infrastructure to ensure it does not harm other States).

128. *See, e.g.*, Cohan, *supra* note 41, at 944 ("[T]he concept of sovereignty . . . has previously been characterized as the right of a State to exercise supreme power over its territory and citizens, free from outside interference."); von Heinegg, *supra* note 7, at 132 ("Moreover, according to the principles of

assertion have often been contested, including in a seminal case decided by the Permanent Court of International Justice (PCIJ), the precursor to the ICJ. In *S.S. "Lotus"*, a dispute arose between France and Turkey over Turkey's assertion of authority in the case of an accidental collision at sea.[129] The Court in that case determined that the public international law regime was fundamentally permissive and that where there was no positive restriction, sovereigns were generally free to assert their authority over individuals in the absence of a specific proscription from doing so.[130]

While that specific decision of the PCIJ has been limited under modern international law,[131] a State's current ability to exercise sovereignty applies to all legal persons within its territory and some outside its territory, such as its citizens who are abroad.[132] This means that a State's sovereign rights and obligations extend to both State and non-State actors who meet those qualifications.

1. Rights

Sovereign States' ability to exercise prescriptive jurisdiction (territorial,[133] nationality,[134] protective,[135] passive personality,[136] and universal[137]) over both State and non-State actors is guided by international law.[138] These accepted limitations represent the modern constraints on the assertion of such jurisdiction.[139] Conflicting

---

active and passive nationality, a State is entitled to exercise its jurisdiction over the conduct of individuals that occurred outside its territory.")

129. S.S. "Lotus" (Fr. v. Turk.), Judgment, 1927 P.C.I.J. (ser. A) No. 10, at 5 (Sept. 7).

130. *Id.* at 18 ("International law governs relations between independent States. The rules of law binding upon States therefore emanate from their own free will as expressed in conventions or by usages generally accepted as expressing principles of law and established in order to regulate the relations between these co-existing independent communities or with a view to the achievement of common aims. Restrictions upon the independence of States cannot therefore be presumed.").

131. *See* U.N. Convention on the Law of the Sea, *supra* note 54, art. 97 ("In the event of a collision or any other incident of navigation concerning a ship on the high seas, involving the penal or disciplinary responsibility of the master or of any other person in the service of the ship, no penal or disciplinary proceedings may be instituted against such person except before the judicial or administrative authorities either of the flag State or of the State of which such person is a national.").

132. *See* Helen Stacy, *Relational Sovereignty*, 55 STAN. L. REV. 2029, 2050–51 (2003) ("Sovereignty attaches itself to the people of the state, not merely the state itself . . . . Relational sovereignty places a higher obligation on the sovereign state to care for and regulate the behavior of its citizens both inside and outside state borders.").

133. RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW § 402(1) (1986).

134. *Id.* § 402(2).

135. *Id.* § 402(3) & cmt. f.

136. *Id.* § 402 & cmt. g.

137. *Id.* § 404.

138. *See* INT'L BAR ASS'N, REPORT OF THE TASK FORCE ON EXTRATERRITORIAL JURISDICTION 11 (2009) ("The starting point for jurisdiction is that all states have competence over events occurring and persons (whether nationals, residents or otherwise) present in their territory. . . . In addition, states have long recognised the right of a state to exercise jurisdiction over persons or events located outside its territory in certain circumstances, based on the effects doctrine, the nationality or personality principle, the protective principle or the universality principle.").

139. *See id.* at 11–16 (discussing the different bases for a State's exercise of extraterritorial jurisdiction).

assertions are normally resolved through the principles of comity.[140] As the U.S. Supreme Court recently described it, "[American] courts have long held that application of [American] antitrust laws to foreign anticompetitive conduct is nonetheless reasonable, and hence consistent with principles of prescriptive comity, insofar as they reflect a legislative effort to redress domestic antitrust injury that foreign anticompetitive conduct has caused."[141]

States have also established international agreements that have created methodologies for the exercise of jurisdiction over persons. These agreements include both multilateral agreements such as the European Cybercrime Convention[142] and bilateral agreements such as extradition treaties.[143] They provide a mechanism for sovereign States to assert rights over individuals in situations of conflicting claims.[144]

2. Obligations

The ability to exercise rights of legal persons also brings obligations to do so. Recall the maxim that States must prevent their territory from knowingly being used to harm the territory of another. That harm is almost always generated by some actor, taking some action. If States have the obligation to prevent known trans-boundary harm, they have to accept the corresponding obligation to exercise control and authority over those within their power who are causing that trans-boundary harm. This obligation applies to both State and non-State actors.

The ICJ provided insight into the application of this obligation to non-State actors in *Armed Activities on the Territory of the Congo*.[145] The Court was unwilling to assign responsibility to Zaire for not preventing the activities of certain armed groups because the government was not capable of doing so.[146] However, the clear implication of the Court's decision is that if the government had been capable, it would have had the obligation to do so.

---

140. Robert C. Reuland, Hartford Fire Insurance Co., *Comity and the Extraterritorial Reach of United States Antitrust Laws*, 29 TEX. INT'L L.J. 159, 161 (1994) ("In adopting a position that comity considerations may be relevant only in the case of a 'true conflict,' the Supreme Court effectively closes the door to the consideration of comity issues under any circumstances short of an actual conflict between U.S. and foreign law.").

141. F. Hoffmann-La Roche Ltd. v. Empagran S.A., 542 U.S. 155, 165 (2004) (emphasis omitted).

142. Convention on Cybercrime, *supra* note 92.

143. *E.g.*, Extradition Treaty between the United States of America and the United Kingdom of Great Britain and Northern Ireland, U.S.-U.K., Mar. 31, 2003, T.I.A.S. No. 07-426.

144. *See, e.g.*, Cohan, *supra* note 41, at 939–40 ("Membership in the United Nations and in other international organizations means that the participating state accepts the right of its fellow members to intervene in its domestic affairs if it has failed in its most fundamental obligations to protect its own citizens . . . ." (internal quotation marks omitted)); Worth, *supra* note 48, at 256 ("Article 12(2)(b) [of the Rome Statute] states that the Court will have personal (*ratione personae*) jurisdiction over the citizens of states that have become party to the [International Criminal Court].").

145. Armed Activities on the Territory of the Congo (Dem. Rep. Congo v. Uganda), Judgment, 2005 I.C.J. 168, paras. 299–301 (Dec. 19).

146. *Id.*

C. *Application to Cyberspace*

One of the potential difficulties with applying sovereignty to cyberspace is the claim that cyberspace is a virtual world and does not lie within any national sovereignty.[147] In other words, skeptics claim that the activities that take place in cyberspace do not always fall under a State's jurisdiction.[148] The next two Subparts will analyze these arguments with respect to territory and persons.

1. Territory

Some have likened cyberspace to the commons, such as the high seas, and proposed that a similar legal regime should apply.[149] The argument is that because cyberspace does not fall within any State's territory, it is not subject to any State's sovereignty.[150] The authors of the *Tallinn Manual* responded to this issue by arguing that "although no State may claim sovereignty over cyberspace *per se*, States may exercise sovereign prerogatives over any cyber infrastructure located on their territory, as well as activities associated with that cyber infrastructure."[151]

Cyber infrastructure is composed of servers, computers, cable, and other physical components.[152] These components are not located in cyberspace, but on some State's territory. It seems clear that a State has jurisdiction and exercises sovereign authority over these components that are located within its territorial boundaries. A State also exercises jurisdiction over cyber infrastructure outside its geographic boundaries if it exercises exclusive control over that cyber infrastructure, such as with cyber infrastructure on a State warship on the high seas.[153] The scope of territorial sovereignty in cyberspace includes the cyber infrastructure "located on a State's land area, in its internal waters, territorial sea and, where applicable, archipelagic waters, and in national airspace" but does not extend to its exclusive economic zone or on the continental shelf where States only exercise "sovereign rights."[154]

The law is at least settled enough with respect to cyber activities that the authors of the *Tallinn Manual* listed as its first "black letter" rule, "A State may exercise control over cyber infrastructure and activities within its sovereign

147. *See* David R. Johnson & David Post, *Law and Borders—The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367, 1371 (1996) ("The power to control activity in Cyberspace has only the most tenuous connections to physical location.").

148. *See, e.g., Id.* at 1372 (arguing that "efforts to control the flow of electronic information across physical borders . . . are likely to prove futile").

149. *See, e.g.*, Dan Hunter, *Cyberspace as Place and the Tragedy of the Digital Anticommons*, 91 CALIF. L. REV. 439, 517 (2003) ("[W]ith the intangible property of cyberspace, we can throw out our normal assumptions about private ownership of the resources and recognize that a commons system might be the most efficient use of the resource.").

150. *See* Johnson & Post, *supra* note 147, at 1370 ("The Net thus radically subverts the system of rule-making based on borders between physical spaces, at least with respect to the claim that Cyberspace should naturally be governed by territorially defined rules.").

151. TALLINN MANUAL r. 1 cmt. 1.

152. *Id.* gloss.

153. *Id.* r. 5.

154. von Heinegg, *supra* note 7, at 128 & n.17.

territory."[155] One of the *Tallinn* authors has also written that "State practice provides sufficient evidence that components of cyberspace are not immune from territorial sovereignty nor from the exercise of State jurisdiction."[156] Nor does connecting that infrastructure to the World Wide Web connote some kind of waiver of sovereignty.[157] In fact, the practice of States is just the opposite—the practice of States has made it clear that they will continue to exercise territorial sovereignty over their cyber infrastructure.[158]

This authority comes with corresponding duties and obligations. One of the primary obligations is that a State has an obligation not to knowingly allow its cyber infrastructure within its territory or under its exclusive control to cause trans-boundary harm.[159] This obligation has been accepted to apply to radio telecommunications[160] and was recently recognized as a rule by the authors of the *Tallinn Manual*.[161]

This obligation has also been stated in multiple official State comments. For example, according to China, sovereign States "have the responsibilities and rights to take necessary management measures to keep their domestic cyberspace and related infrastructure free from threats, disturbance, attack and sabotage."[162] Similarly, India has stated,

> By creating a networked society and being a part of [a] global networked economy, it is necessary for nation states to realise that they not only have a requirement to protect their own ICT infrastructure but at the same time have a responsibility to ensure that their ICT is not abused, either covertly or overtly, by others to target or attack the ICT infrastructure of another nation state.[163]

Likewise, Russia has stated that "States and other subjects of international law should refrain of [sic] such actions against each other and should bear responsibility at international level for such actions in information space, carried out directly, under their jurisdiction or in the framework of international organizations of their membership."[164] Finally, the U.S. government's 2011 International Strategy for Cyberspace calls on States to "recognize the international implications of their technical decisions, and act with respect for one another's networks and the broader Internet."[165]

---

155. TALLINN MANUAL r. 1.

156. von Heinegg, *supra* note 7, at 126.

157. *Id.*

158. DEPARTMENT OF DEFENSE, STRATEGY FOR OPERATING IN CYBERSPACE, *supra* note 89, at 1.

159. Schmitt, *The Law of Cyber Warfare*, *supra* note 12, at 276.

160. *Developments in the Field of Information and Telecommunications*, *supra* note 8, at 3.

161. TALLINN MANUAL.

162. Kanuck, *supra* note 9, at 1591 (internal quotation marks omitted).

163. *Id.*

164. *Id.* at 1591 n.88.

165. OFFICE OF THE PRESIDENT, INTERNATIONAL STRATEGY FOR CYBERSPACE, *supra* note 37, at 10.

These and similar statements, combined with limited State practice, have led many commentators[166] to argue,

> States have an affirmative duty to prevent cyberattacks from their territory against other states. This duty actually encompasses several smaller duties, to include passing stringent criminal laws, conducting vigorous investigations, prosecuting attackers, and, during the investigation and prosecution, cooperating with the victim-states of cyberattacks that originated from within their borders.[167]

The kinds of acts that equate to trans-boundary harm might include attacks on networks, exploitation of networks, and other hostile acts in cyberspace that threaten peace and stability, civil liberties and privacy.[168] At this point, it is still unclear under the law as to whether the mere transit of data through a particular nation's infrastructure rises to the level of a prohibited activity, even if the data eventually results in harm to another State.[169]

Note that the obligation only triggers if the State from whose territory the harm originates has knowledge of the harm.[170] When States have knowledge of the harmful acts, they have a duty to stop them.[171] Knowledge might be imputed to the State if State agents or organs, such as intelligence or law enforcement agencies, know of the harm emanating from the State's cyber infrastructure, even if those agents or organs choose to not inform other agencies in the government.[172]

There may also be times when neither a State nor its organs or agents have actual knowledge but should have had knowledge, given the circumstances. In the ICJ's *Corfu Channel* case, the court held Albania liable for harm to England, even though there was no direct evidence that Albania knew of the harm. In that case, the court concluded that given the circumstances, Albania must have known about the emplacement of the mines that caused the harm.[173] The "must have known" standard is higher than a "should have known" standard but demonstrates that proving actual knowledge is not required. As for States who "should have known," international law is still unclear as to the obligation of such a State.[174] However, von Heinegg is willing to allow a rebuttable presumption of actual or constructive knowledge if "a cyber attack has been launched from cyber infrastructure that is

166. *E.g.*, David E. Graham, *Cyber Threats and the Law of War*, 4 J. NAT'L SEC. L. & POL'Y 87, 93–94 (2010); Matthew J. Sklerov, *Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defenses against States Who Neglect Their Duty to Prevent*, 201 MIL. L. REV. 1, 62–63 (2009).

167. Sklerov, *supra* note 166, at 62–63.

168. *See* OFFICE OF THE PRESIDENT, INTERNATIONAL STRATEGY FOR CYBERSPACE, *supra* note 37, at 12–14 (recognizing that cyberspace activities can have effects beyond borders and detailing initiatives that will be undertaken to protect the United States against threats posed by cyber criminals or States and their proxies).

169. von Heinegg, *supra* note 7, at 137.

170. *Id.* at 136.

171. *Id.* at 135–36.

172. *Id.* at 136.

173. Corfu Channel (U.K. v. Alb.), Judgment, 1949 I.C.J. 4, 19–20 (Apr. 9).

174. *See* von Heinegg, *supra* note 7, at 151 (speculating hypothetically about whether constructive knowledge is sufficient to establish a violation).

under exclusive government control and that is used only for non-commercial government purposes."[175]

There is currently an ongoing discussion as to whether a State's responsibility to prevent knowing cyber harm creates a duty to monitor networks in order to "know" when cyber harms exist.[176] In other words, if such a responsibility exists, if State A knows that its infrastructure is being used to cause trans-boundary harm to State B, State A has an obligation to stop the harm.[177] In order to effectively comply with that obligation, there is an emerging norm that State A has an obligation to monitor its cyber infrastructure and take proactive measures to prevent harm from emanating from cyber infrastructure over which State A exercises sovereignty.[178] However, this emerging norm is still quite controversial, particularly when considered in light of potential human rights obligations that might be compromised in the process of monitoring.[179]

Until that norm becomes generally accepted, target States will have to find ways to determine the level of knowledge of States from whose territory harmful cyber effects originate before allocating responsibility. In the current view of the United States,

> [Department of Defense (DoD)] adheres to well-established processes for determining whether a third country is aware of malicious cyber activity originating from within its borders. In doing so, DoD works closely with its interagency and international partners to determine: [(1)] The nature of the malicious cyber activity; [(2)] The role, if any, of the third country; [(3)] The ability and willingness of the third country to respond effectively to the malicious cyber activity; and [(4)] The appropriate course of action for the U.S. Government to address potential issues of third-party sovereignty depending upon the particular circumstances.[180]

In addition to the obligation to prevent trans-boundary harm, a State has an obligation to cooperate with the victim State in the event of adverse or unlawful cyber effects from cyber infrastructure located in its territory or under its exclusive governmental control when it may affect international peace and security.[181] A

---

175. *Id.* at 137. Note that von Heinegg clearly states that the presumption does not allow for attribution. *Id.*

176. *See generally* Jensen, *State Obligations*, *supra* note 127.

177. *See id.* at 13 (stating that in order to comply with the duty to control their cyber infrastructures, States have an emerging duty to monitor cyber activities within their territories in order to prevent or stop activities that are adversely or unlawfully affecting other States).

178. *Id.*

179. *Cf.* EKATERINA A. DROZDOVA, CIVIL LIBERTIES AND SECURITY IN CYBERSPACE 13 (2000), *available at* http://fsi.stanford.edu/sites/default/files/drozdova.pdf ("While a system for advanced monitoring, searching, tracking, and analyzing of communications may be very helpful against cyber crime and terrorism, it would also provide participating governments, especially authoritarian governments or agencies with little accountability, tools to violate civil liberties domestically and abroad.").

180. DEPARTMENT OF DEFENSE, CYBERSPACE POLICY REPORT, *supra* note 105, at 8.

181. In addition to those circumstances mentioned above where the maintenance of international

State may also have a treaty obligation to establish criminal information sharing and criminal processing arrangements as a matter of domestic law.[182]

This obligation to cooperate is based on the U.N. Charter[183] and ICJ opinions,[184] and is also confirmed in the U.N. General Assembly's Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in Accordance with the Charter of the United Nations.[185] The obligation to cooperate with respect to cyber incidents is also enshrined in the European Convention on Cybercrime, which has forty-two States parties and an additional eleven signatory States.[186]

This norm of cooperation only requires States to cooperate when the adverse or unlawful cyber incident originates from infrastructure within the territory or under its exclusive governmental control or when the unlawful cyber incident transits the cyber infrastructure in the State's territory or under its exclusive government control. Both conditions must be met for the duty to be applicable. No specific standard for the level of cooperation is clearly agreed upon, but the general consensus is that States must exercise good faith when fulfilling this duty.[187]

As an example, if a cyber incident originates in State A and threatens State B's critical infrastructure such that there is a threat to international peace and security, both State A and State B have a legal duty to cooperate to peacefully resolve that incident.

As with the obligation concerning trans-boundary harm, the obligation to cooperate also has a number of unresolved issues. Most relevant to this Article is the fact that historical State practice does not demonstrate that States accept the obligation to cooperate in any meaningful way.[188] Again, the 2007 situation between

---

peace and security is at risk, the duty to cooperate also applies to the solving of international problems of economic, social, cultural, or humanitarian character. U.N. Charter art. 1, para. 3. States also have a duty to cooperate in scientific investigation in Antarctica. The Antarctic Treaty, *supra* note 53, art. 2. The duty to cooperate also applies to the scientific investigation of outer space. Outer Space Treaty, *supra* note 55, art. 1. Finally, international cooperation applies to marine scientific research. U.N. Convention on the Law of the Sea, *supra* note 54, art. 143.

182. *See, e.g.*, Convention on Cybercrime, *supra* note 92, art. 26, para. 1 ("A Party may, within the limits of its domestic law and without prior request, forward to another Party information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings concerning criminal offences established in accordance with this Convention or might lead to a request for co-operation by that Party under this chapter.").

183. U.N. Charter art. 1, paras. 1, 3; *Id.* art. 33, para. 1.

184. *See, e.g.*, Pulp Mills on the River Uruguay (Arg. v. Uru.), Judgment, 2010 I.C.J. 14, para. 102 (Apr. 20) (finding it vital for parties to comply with their procedural obligations under the 1975 Statute of the River Uruguay because cooperation is essential to the protection of the river).

185. G.A. Res. 2625 (XXV), *supra* note 80, at 123.

186. Article 23 requires that "[t]he Parties shall co-operate with each other" and provide mutual assistance, particularly with respect to investigations of cyber incidents. Convention on Cybercrime, *supra* note 92, art. 23.

187. *See* Kotzur, *supra* note 93, para. 16 ("One of the most basic principles governing the creation and performance of legal obligations, whatever their source, is the principle of good faith.").

188. *See* Schmitt, *The Law of Cyber Warfare*, *supra* note 12, at 273 ("A state's national interests undergird its consent or conduct .... States might seek, for example, to maximize power and influence at the expense of other states ....").

Estonia and Russia is instructive. Estonia found Russia's response to its queries and requests for assistance unhelpful and protective of Russian interests.[189]

2. Persons

The U.S. Department of Justice's recent indictment of five members of the Chinese Army for cyber hacking[190] represents a significant shift from the methodology States have traditionally used in dealing with State-sponsored cyber activities.[191] For the United States to move away from its normal diplomatic approach[192] and invoke domestic criminal law as a means of deterring State-sponsored cyber activities is a definite policy shift.[193] Certainly, it is improbable that the indictment will result in any convictions as China and the United States do not have an extradition treaty[194] and China has signaled no intention to honor such a request anyway. However, the idea that States will use domestic criminal law as a tool to deter other States who are engaged in harmful cyber activities is a potentially interesting development. The use of criminal law for non-State actors, on the other hand, is the norm, however ineffective.

It seems clear that in addition to State actors, "terrorist groups and even individuals, [sic] now have the capability to launch cyber-attacks, not only against military networks, but also against critical infrastructures that depend on computer

189. See Ruus, *supra* note 2 ("[T]he Estonian State Prosecutor made a formal investigative assistance request, which Moscow rejected, alleging that procedural problems prevented cooperation.").

190. Michael S. Schmidt & David E. Sanger, *5 in China Army Face U.S. Charges of Cyberattacks*, N.Y. TIMES, May 19, 2014, http://www.nytimes.com/2014/05/20/us/us-to-charge-chinese-workers-with-cyberspying.html. China is, of course, not the only State conducting cyber activities. Recent media revelations concerning the United States' cyber activities have alleged widespread actions against both State and commercial entities. Simon Romero & Randal C. Archibold, *Brazil Angered Over Report N.S.A. Spied on President*, N.Y. TIMES, Sept. 2, 2013, http://www.nytimes.com/2013/09/03/world/americas/brazil-angered-over-report-nsa-spied-on-president.html; David E. Sanger & Nicole Perlroth, *N.S.A. Breached Chinese Servers Seen as Security Threat*, N.Y. TIMES, Mar. 22, 2014, http://www.nytimes.com/2014/03/23/world/asia/nsa-breached-chinese-servers-seen-as-spy-peril.html; *Snowden NSA: Germany to Investigate Merkel "Phone Tap"*, BBC (June 4, 2014), http://www.bbc.com/news/world-europe-27695634; Jonathan Watts, *NSA Accused of Spying on Brazilian Oil Company Petrobras*, GUARDIAN, Sept. 9, 2013, http://www.theguardian.com/world/2013/sep/09/nsa-spying-brazil-oil-petrobras.

191. *See* Schmidt & Sanger, *supra* note 190 ("[President Obama and Defense Secretary Chuck Hagel] have attempted to engage the Chinese in a dialogue over norms for operating in cyberspace, a careful diplomatic dance that has gone on for several years. But Monday's action by the Justice Department marked an attempt to publically shame the Liberation Army . . . .").

192. *See* Ellen Nakashima, *U.S. Publicly Calls on China to Stop Commercial Cyber-Espionage, Theft of Trade Secrets,* WASH. POST, Mar. 11, 2013, http://www.washingtonpost.com/world/national-security/us-publicly-calls-on-china-to-stop-commercial-cyber-espionage-theft-of-trade-secrets/2013/03/11/28b21d12-8a82-11e2-a051-6810d606108d_story.html (discussing the United States' diplomatic efforts to hold China accountable for cyber-espionage).

193. *See* Schmidt & Sanger, *supra* note 190 (describing how the Justice Department indicted five members of the Chinese People's Liberation Army and illustrating how this represents a U.S. policy shift on dealing with Chinese cyber activities).

194. Dominic Rushe, *Chinese Hackers Break into US Federal Government Employee Database*, GUARDIAN, July 10, 2014, http://www.theguardian.com/world/2014/jul/10/china-hackers-us-government-employee-database.

networks."[195] And the results of such actions can be catastrophic. "[M]alicious actors, state and non-state, have the ability to compromise and control millions of computers that belong to governments, private enterprises and ordinary citizens."[196] The threat is such that

> [t]he President's May 2011 International Strategy for Cyberspace states that the United States will, along with other nations, encourage responsible behavior and oppose those who would seek to disrupt networks and systems, dissuading and deterring malicious actors, and reserving the right to defend these national security and vital national assets as necessary and appropriate.[197]

The fact that cyber operations may be initiated by a vast array of persons implicates the States from which those persons take those actions. Every time there is a victim-State, there is a State from which the action was initiated and often a State or States through which the activity passed. In each case, those States have not only the right to control their citizens and others who might be involved, but also the obligation to do so.[198] When persons take actions from within a State that harm another State, the State from which the harm originated has an obligation to try to stop those actions, once the State has knowledge.[199] If a State is monitoring its networks and knows in advance, it can act preemptively to stop that activity before it emanates from within its sovereign territory. Additionally, as stated above with respect to controlling actions, a State can take proactive measures to discourage non-State actors by "passing stringent criminal laws, conducting vigorous investigations, prosecuting attackers, and, during the investigation and prosecution, cooperating with the victim-States of cyberattacks that originated from within their borders."[200]

D. The Way Ahead

Applying a State's sovereign rights and obligations to persons with respect to cyber activities emphasizes the key role States must play in the way ahead for cyberspace. As the community of States moves forward, States will have to determine how the exercise of those sovereign rights and obligations can best be managed to accomplish each State's purposes.

For example, there are a number of issues revolving around the obligation to prevent trans-boundary harm. One of these issues stems from the fact that international law allows for some *de minimis* imposition on the rights of other States.[201] It is unclear generally what the limit of acceptable *de minimis* harm is, but

195. Liaropoulos, *supra* note 9, at 136 (citation omitted).

196. *Id.* at 137.

197. DEPARTMENT OF DEFENSE, CYBERSPACE POLICY REPORT, *supra* note 105, at 2.

198. Jensen, *Sovereignty and Neutrality*, *supra* note 9, at 826–27.

199. *Id.*

200. Sklerov, *supra* note 166, at 62.

201. *See* Jutta Brunnée, *Sic utere tuo ut alienum non laedas*, *in* MAX PLANCK ENCYCLOPEDIA OF PUBLIC INTERNATIONAL LAW para. 7 (2010) ("[T]he mere causation of transboundary harm does not transgress the *sic utere tuo* maxim.").

this is particularly unclear in cyberspace, where it is accepted that most cyber activities will not rise to the level of a use of force.[202] As time progresses, State practice will indicate what the acceptable amount of *de minimis* harm is and where that line is generally crossed. Currently, that line is quite high because States are unwilling to respond in forceful ways to cyber activities.[203] The shift in U.S. policy to apply domestic criminal remedies reflects that at least some States are not comfortable with the current paradigm. States' willingness to accept State-sponsored cyber activities, even those that are far below the use of force, seems to be waning. The future will undoubtedly bring more proactive measures to deter States from conducting cyber activities and reduce the acceptable level of *de minimis* cyber harm.

Another current issue that will likely come to the fore in the near future concerns the knowledge requirement for the trans-boundary harm obligation. While the law is clear that some form of knowledge, whether actual or constructive, is required for responsibility, the law is unclear as to the responsibility of a State that chooses not to invest in cyber capabilities on purpose, in an effort to remain blind to its obligations.[204] This issue of the level of knowledge, and responsibility to seek knowledge, will need to be resolved by State practice over time. As the duty to monitor and prevent continues to emerge, States will have to accept greater responsibility under a constructive knowledge standard and a State's ability to practice willful blindness will disappear. The pressures of the increasing availability of technology and the rising awareness of cyber activities will aid in this movement.

Finally, though there is a clearly recognized rule of international law on the acceptance of responsibility for trans-boundary harm, State practice in the cyber area has been inconsistent at best, and directly non-compliant in many cases.[205] Particularly in the area of cyber operations that are generated from within a State's borders, there is a mixed history on responsible States' willingness to accept responsibility.[206] Though this trend could actually go either way, it seems likely that the harms that are possible through cyber activities will eventually outweigh the benefits that States accrue by having freedom of action. Thus, particularly in light of the fact that non-State actors and even lone individuals can harness State-level violence through the use of cyber tools, States will soon find it in their best interest

202. *See* TALLINN MANUAL r. 11 (defining the term "use of force" in the cyber context as an operation the scale and effects of which are comparable to non-cyber operations that would qualify as a use of force).

203. *But see* DEPARTMENT OF DEFENSE, CYBERSPACE POLICY REPORT, *supra* note 105, at 4 ("Finally, the President reserves the right to respond using all necessary means to defend our Nation, our Allies, our partners, and our interests from hostile acts in cyberspace. Hostile acts may include significant cyber attacks directed against the U.S. economy, government or military. As directed by the President, response options may include using cyber and/or kinetic capabilities provided by [the Department of Defense].").

204. TALLINN MANUAL r. 93.

205. *See, e.g.*, discussion *supra* Part II.C.1 on Russia's unwillingness to assist Estonia after the 2007 cyber attacks.

206. *See, e.g.*, Sklerov, *supra* note 166, at 10 ("As may be expected, China and Russia reject these accusations.").

to regulate themselves in order to protect themselves not only from other States, but from non-State actors as well.

CONCLUSION

An analysis of the international doctrine of State sovereignty demonstrates that many of those norms are directly applicable to cyber operations and can easily be applied with respect to States. In fact, the recently published *Tallinn Manual* concludes that principles of sovereignty can be applied and does so apply them.[207]

However, there are still areas where State practice has presented difficulties, such as the area of accepting responsibility for trans-boundary harm, the emerging principles of a duty to monitor and prevent, and the duty to apply due regard to a State's cyber activities.

It seems clear, though, that the future will provide greater clarity as incidents of state cyber activities become more widespread and the information more available to the public. At that point, the way ahead is likely to demonstrate that the doctrine of sovereignty continues to apply to cyber operations.

207. TALLINN MANUAL R. 1.

Toward a Global Cybersecurity Standard of Care?: Exploring the Implications of the 2014 NIST Cybersecurity Framework on Shaping Reasonable National and International Cybersecurity Practices

SCOTT J. SHACKELFORD, JD, PHD*; ANDREW A. PROIA, JD**; BRENTON MARTELL, JD***; & AMANDA N. CRAIG, MSC, JD****

ABSTRACT

Even though U.S. congressional and multilateral efforts aimed at enhancing cybersecurity have thus far largely failed in their aims, courts and regulators are using existing common law doctrines and statutory enactments to hold companies accountable for cyber attacks. However, such judicial and regulatory actions have often been haphazard, due in part to confusion over what constitute reasonable standards of cybersecurity care. This Article analyzes the emerging cybersecurity duty of care and examines the potential impact of the 2014 National Institute of Standards and Technology (NIST) Cybersecurity Framework on shaping reasonable standards of cybersecurity. Given that cybersecurity best practices are not yet well defined, the NIST Framework has the potential to shape standards not only for critical infrastructure firms but also for the private sector writ large. Indeed, the Federal Communications Commission (FCC) in November 2013 wrote that it plans "to use an emerging framework of cybersecurity standards to assess and prioritize best practices . . . to address evolving cyber threats" in the telecommunications industry.[1] Moreover, the NIST Framework has the potential to shift the

* Assistant Professor of Business Law and Ethics, Indiana University; Senior Fellow, Center for Applied Cybersecurity Research; Distinguished Visiting Fellow, Notre Dame Institute for Advanced Study; Edward Teller National Fellow, Hoover Institution, Stanford University.

** JD, Indiana University Maurer School of Law; Postdoctoral Fellow, Indiana University Center for Applied Cybersecurity Research.

*** JD, Indiana University Maurer School of Law.

**** Senior Cybersecurity Strategist, Microsoft Corporation; MsC, University of Oxford; JD, Indiana University Maurer School of Law.

1. FCC, *Telecom Industry Plan to Map Current Best Practices to NIST Framework*, INSIDE CYBERSECURITY (Nov. 20, 2013), http://insidecybersecurity.com/index.php?option=com_user&view=login&return=aHR0cDovL2luc2lkZWN5YmVyc2VjdXJpdHkuY29tL0N5YmVyLURhaWx5LU5ld3MvRGFpbHktTmV3cy9mY2MtdGVsZWNvbS1pbmR1c3RyeS1wbGFuLXRvLW1hcC1jdXJyZW50LWJlc3QtcHJhY3RpY2VzLXRvLW5pc3QtZnJhbWV3b3JrL2llbnUtaWQtMTA3NS5odG1s [hereinafter FCC,

cybersecurity landscape internationally, especially in jurisdictions that largely favor a voluntary approach to enhancing cybersecurity, including the United Kingdom, India, and to a lesser extent, the European Union. The uptake of the NIST Framework beyond the United States could help to foster a global standard of cybersecurity care, promoting consistency, benefitting businesses active across jurisdictions, and contributing to cyber peace.

SUMMARY

Telecom Industry].

INTRODUCTION

> The national and economic security of the United States depends on the reliable functioning of critical infrastructure. Cybersecurity threats exploit the increased complexity and connectivity of critical infrastructure systems, placing the Nation's security, economy, and public safety and health at risk. Similar to financial and reputational risk, cybersecurity risk affects a company's bottom line. It can drive up costs and impact revenue. It can harm an organization's ability to innovate and to gain and maintain customers.
>
> – Executive Summary, NIST Cybersecurity Framework[2]

During the winter of 2013–2014, amidst the school delays and extreme weather conditions in much of the United States,[3] the federal Emergency Alert System issued a warning, but perhaps not the one people expected: "Civil authorities in your area have reported that the bodies of the dead are rising from their graves and attacking the living .... Do not attempt to approach or apprehend these bodies, as they are considered extremely dangerous."[4] Hackers had penetrated the System to issue a "bogus zombie alert" in yet another episode showcasing the myriad vulnerabilities buried in "critical systems throughout [U.S.] government."[5] Aside from being fodder for bored hackers, such weaknesses can be exploited by cyber criminals, terrorists, and nation States, which makes securing "critical infrastructure" a key test of effective cybersecurity policymaking.[6] Thus far, though, it is a test that many nations, including the United States, the United Kingdom, and India, are failing.

---

2. NAT'L INST. OF STANDARDS & TECH., U.S. DEP'T OF COMMERCE, FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY 1 (2014) [hereinafter NIST CYBERSECURITY FRAMEWORK].

3. *See National Overview—February 2013*, NOAA (Mar. 2013), http://www.ncdc.noaa.gov/sotc/national/2013/2 ("Three major winter storms impacted the nation during February, contributing to an above-average monthly snow cover ...."). Note that sections of this material are adapted from SCOTT J. SHACKELFORD, MANAGING CYBER ATTACKS IN INTERNATIONAL LAW, BUSINESS, AND RELATIONS: IN SEARCH OF CYBER PEACE (2014) [hereinafter SHACKELFORD, MANAGING CYBER ATTACKS].

4. Craig Timberg & Lisa Rein, *Senate Cybersecurity Report Finds Agencies Often Fail to Take Basic Preventive Measures*, WASH. POST, Feb. 4, 2014, http://www.washingtonpost.com/business/technology/senate-cybersecurity-report-finds-agencies-often-fail-to-take-basic-preventive-measures/2014/02/03/493390c2-8ab6-11e3-833c-33098f9e5267_story.html (omission in original).

5. *Id.*

6. *E.g.*, Exec. Order No. 13636, 78 Fed. Reg. 11739, 11739 (Feb. 19, 2013) ("[C]ritical infrastructure

The growing danger posed by seemingly ever-more sophisticated and plentiful cyber attackers, especially as it relates to securing critical infrastructure, is not news. For example, former National Security Agency (NSA) and U.S. Cyber Command chief General Keith Alexander told a Senate committee in June 2013 that "'[o]n a scale of one to 10, with 10 being strongly defended, our critical infrastructure's preparedness to withstand a destructive cyber attack is about a three based on my experience.'"[7] Similarly, the lack of progress—not only in Congressional efforts, as seen in the debates surrounding the Cybersecurity Act of 2012,[8] but also in international efforts aimed at managing cyber attacks—is well documented.[9] This lack of regulatory engagement has often left judges in an uncertain position about what steps companies, including those operating critical infrastructure, should take to secure their data and systems.[10] A lack of definition regarding what constitutes a standard of care in the cybersecurity context has been the result. Enter the Obama Administration.

In February 2013, President Obama issued an executive order that, among other things, expanded public-private information sharing and tasked the NIST with establishing a voluntary "Cybersecurity Framework" comprised partly of private-sector best practices that companies could adopt to better secure critical infrastructure.[11] The Framework version 1.0, Framework for Improving Critical Infrastructure Cybersecurity, was released in February 2014.[12] The Cybersecurity Framework "harmonizes consensus standard and industry best practices to provide, its proponents argue, a flexible and cost-effective approach to enhancing cybersecurity that assists owners and operators of critical infrastructure in assessing and managing cyber risk."[13] The Framework provides a voluntary procedure to map cybersecurity best practices, determine the overall state of an organization's cyber

---

means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.").

7. *NSA Chief Says U.S. Infrastructure Highly Vulnerable to Cyber Attack*, REUTERS, June 12, 2013, http://www.reuters.com/article/2013/06/12/us-usa-cybersecurity-idUSBRE95B10220130612.

8. *See, e.g.*, Scott J. Shackelford, Essay, *In Search of Cyber Peace: A Response to the Cybersecurity Act of 2012*, 64 STAN. L. REV. ONLINE 106, 109–10 (2012) (discussing congressional efforts around the Cybersecurity Act of 2012). *But see U.S. Senators Push Ahead with Cybersecurity Legislation*, REUTERS, June 17, 2014, http://www.reuters.com/article/2014/06/17/us-usa-cybersecurity-congress-idUSKBN0ES29N 20140617 (discussing the expectation of Congressional cybersecurity enactments).

9. *See, e.g.*, Tom Gjelten, *Seeing the Internet as an 'Information Weapon'*, NPR (Sept. 23, 2010), http://www.npr.org/templates/story/story.php?storyId=130052701 (discussing the fact that United Nations-sponsored cyber disarmament discussions have been ongoing since the late 1990s without much to show for it); Tony Romm, *Cybersecurity in Slow Lane One Year after Obama Order*, POLITICO, Feb. 9, 2014, http://www.politico.com/story/2014/02/cybersecurity-in-slow-lane-one-year-after-obama-order-103307.html ?hp=f1 ("Nearly a year after President Barack Obama issued an executive order to improve the cybersecurity of the nation's vital assets, the administration doesn't have much to show: The government is about to produce only some basic standards, with little incentive for the private sector to participate.").

10. *See* Guin v. Brazos Higher Educ. Serv., No. Civ. 05-668 RHK/JSM, 2006 WL 288483, at *4 (D. Minn. Feb. 7, 2006) (dealing with the difficulties associated with applying negligence to cases involving cyber security).

11. Exec. Order No. 13636, 78 Fed. Reg. at 11740–41.

12. NIST CYBERSECURITY FRAMEWORK, *supra* note 2.

13. Scott J. Shackelford & Andrew Proia, *Why Ignoring the NIST Framework Could Cost You*, HUFFINGTON POST (May 2, 2014), http://www.huffingtonpost.com/scott-j-shackelford/why-ignoring-the-nist-fra_b_5244112.html.

risk management practices, and structure roadmaps for organizations to mitigate those risks.[14]

To date, responses to the Framework have been mixed. Some, for instance, have argued that the Framework "represents the best efforts of the administration and . . . industry representatives from the 16 critical infrastructure sectors to work together to address a threat which President Obama has called one of the gravest national security dangers the United States faces."[15] Indeed, since its release, the Framework has garnered support from state and federal legislators, business executives, and public interest organizations.[16] However, praise has not been universal. Some, for example, have cautioned that the Framework does not go far enough in terms of its scope, influence, and impact.[17] One of the main questions surrounding the NIST Framework is how "voluntary" it will actually turn out to be—as well as how voluntary it should be.[18]

From its inception, the Framework has been developed with an aim toward creating a cost-effective method of addressing critical infrastructure cybersecurity vulnerabilities without enacting binding (and potentially cumbersome and inflexible) regulatory requirements.[19] Depending on the success of this and other similar programs, the Framework could help establish a baseline "standard of cybersecurity care" that could define legal liability for critical infrastructure organizations prior to

---

14. *See generally* NIST CYBERSECURITY FRAMEWORK, *supra* note 2.

15. Ian Wallace, *Introductory Remarks at the Brookings Institution's Panel Discussion, Improving Critical Infrastructure Cybersecurity: The Cybersecurity Framework and Beyond* (C-SPAN television broadcast Feb. 19, 2014), *available at* http://www.c-span.org/video/?317876-1/critical-infrastructure-cybersecurity-framework/.

16. *See generally* WHITE HOUSE, CYBERSECURITY FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE: WHAT OTHERS ARE SAYING (2014), *available at* http://www.whitehouse.gov/sites/default/files/docs/cybersecurity_framework_-_what_others_are_saying_2_27.pdf (providing statements of approval from various company executives, federal, state, and local governmental officials, and civil society and privacy groups).

17. *See, e.g.*, Mark Clayton, *Why Obama's Executive Order on Cybersecurity Doesn't Satisfy Most Experts*, CHRISTIAN SCI. MONITOR, Feb. 13, 2013, http://www.csmonitor.com/USA/Politics/2013/0213/Why-Obama-s-executive-order-on-cybersecurity-doesn-t-satisfy-most-experts (discussing shortcomings of the Executive Order, including that it failed to stress the importance of its recommendations); Romm, *supra* note 9 ("Nearly a year after President Barack Obama issued an executive order to improve the cybersecurity of the nation's vital assets, the administration doesn't have much to show: The government is about to produce only some basic standards, with little incentive for the private sector to participate.").

18. *See, e.g.*, *NIST's Voluntary Cybersecurity Framework May Be Regarded as De Facto Mandatory*, HOMELAND SECURITY NEWS WIRE (Mar. 3, 2014), http://www.homelandsecuritynewswire.com/dr20140303-nist-s-voluntary-cybersecurity-framework-may-be-regarded-as-de-facto-mandatory (stating that experts have warned that many of the recommendations in the framework "may be used by courts, regulators, and even consumers to hold institutions accountable for failures that could have been prevented if the cybersecurity framework had been fully implemented by the respective institution").

19. The Departments of Homeland Security, Treasury, and Commerce have proposed incentives that could encourage voluntary utilization of the Framework. Michael Daniel, *Incentives to Support Adoption of the Cybersecurity Framework*, WHITE HOUSE BLOG (Aug. 6, 2013), http://www.whitehouse.gov/blog/2013/08/06/incentives-support-adoption-cybersecurity-framework [hereinafter Daniel, *Incentives*]; *see also infra* note 240; Charlie Mitchell, *DHS Tightens Explanation of How Cyber Voluntary Program Will Help Industry*, INSIDE CYBERSECURITY (Feb. 24, 2014), http://insidecybersecurity.com/Cyber-General/Cyber-Public-Content/dhs-tightens-explanation-of-how-cyber-voluntary-program-will-help-industry/menu-id-1089.html (reporting on the promotion of the voluntary C-Cubed program for cybersecurity standards by the Department of Homeland Security).

and following cyber attacks. Currently, no baseline, comprehensive cybersecurity obligations are imposed across all of the U.S. critical infrastructure, but regulations do exist for certain sectors,[20] leaving the status quo a complex patchwork of oftentimes ambiguous state and federal regulations overlaying applicable common law doctrines.[21]

The NIST Framework not only has the potential to shape a standard of care for domestic critical infrastructure organizations but also could help to harmonize global cybersecurity best practices for the private sector writ large.[22] Existing legal literature has yet to delve deeply into shaping a standard of care in the cybersecurity context.[23] This Article fills that niche by analyzing to what extent cybersecurity standards of care are emerging organically and examining the potential impact of the NIST Framework on crystallizing best practices in the United States and beyond.[24] There is some evidence this may in fact already be occurring,[25] including in jurisdictions that favor a largely voluntary approach to enhancing cybersecurity such as the United Kingdom,[26] India,[27] and, to a lesser extent, the European Union (EU).[28]

---

20. EDWARD C. LIU ET AL., CONG. RESEARCH SERV., R42409, CYBERSECURITY: SELECTED LEGAL ISSUES 1–2 (2012).

21. *See* ERIC A. FISCHER, CONG. RESEARCH SERV., R42114, FEDERAL LAWS RELATING TO CYBERSECURITY: OVERVIEW AND DISCUSSION OF PROPOSED REVISIONS 52–61 (2013) (identifying over forty laws with provisions related to cybersecurity).

22. For example, some stakeholders have already argued that any time a "company's cybersecurity practices are [] questioned during a regulatory investigation and litigation, the baseline for what's considered commercially reasonable is likely to become the NIST Cybersecurity Framework." Gerald Ferguson, *NIST Cybersecurity Framework: Don't Underestimate It*, INFORMATIONWEEK (Dec. 9, 2013), http://www.informationweek.com/government/cybersecurity/nist-cybersecurity-framework-dont-underestimate-it/d/d-id/1112978.

23. *Cf.* Stephen E. Henderson & Matthew E. Yarbrough, *Suing the Insecure?: A Duty of Care in Cyberspace*, 32 N.M. L. REV. 11, 17–21 (2002) (arguing for adoption of traditional negligence law principles in the context of information security); Vincent R. Johnson, *Cybersecurity, Identity Theft, and the Limits of Tort Liability*, 57 S.C. L. REV. 255, 260 n.25 (2005) (investigating elements of an emerging duty of care in the identity theft context); Vincent R. Johnson, *Data Security and Tort Liability*, J. INTERNET L., Jan. 2008, at 22, 23–24 [hereinafter Johnson, *Data Security*] (discussing "voluntary assumption of a duty to protect data"); Melanie J. Teplinsky, *Fiddling on the Roof: Recent Developments in Cybersecurity*, 2 AM. U. BUS. L. REV. 225, 301–03 (2013) (discussing recent legislative proposals addressing cybersecurity); Emily Kuwahara, Note, *Tort v. Contracts: Can Microsoft Be Held Liable to Home Consumers for Its Security Flaws?*, 80 S. CAL. L. REV. 997, 1014–15 (2007) (discussing policies behind the standard of care imposed); Kathryn E. Picanso, Note, *Protecting Information Security Under a Uniform Data Breach Notification Law*, 75 FORDHAM L. REV. 355, 377–80 (2006) (examining the duty of care in the information security context).

24. Our focus in this regard is primarily on negligence case law. However, other applicable areas of law including fiduciary duties and statutory compliance will also be examined. For instance, "chemical facilities are subject to chemical facility anti-terrorism standards (CFATS) promulgated by the Department of Homeland Security (DHS), which include provisions requiring chemical facilities to take measures to protect against cyber threats." LIU ET AL., *supra* note 20, at 1–2.

25. *FCC, Telecom Industry*, *supra* note 1, ("The telecommunications industry and the Federal Communications Commission plan to use an emerging framework of cybersecurity standards to assess and prioritize best practices for the sector as it works to address evolving cyber threats . . . .").

26. *E.g.*, Jane Jenkins, *The Network and Information Security Directive—What Role Can Regulation Play in Improving CyberSecurity: The Legal Perspective*, *in* CYBER SECURITY 2.0: REFLECTIONS ON UK/EU CYBER SECURITY CO-OPERATION 10, 11 (2014) ("The UK Government . . . advocates a policy of voluntary information sharing and has therefore set up the information sharing partnership (CISP) to encourage the sharing of information about attacks and the means to combat them.").

27. *FCC, Telecom Industry*, *supra* note 1.

28. *Proposal for a Directive of the European Parliament and of the Council concerning Measures to*

For businesses active across jurisdictions, and depending on the uptake of the NIST Framework by stakeholders, a global standard of cybersecurity care could eventually emerge that would promote consistency and contribute to "cyber peace" even absent regulatory action.[29]

In an effort to explore the past, present, and future development of a cybersecurity standard of care both domestically and globally, this Article is structured as follows: Part I sets the stage by analyzing the current state of U.S. law shaping a cybersecurity duty of care. Part II then lays out the NIST Framework, discussing its origins and evolution. Finally, Part III applies the findings from Part II to the legal doctrines revealed in Part I in an effort to hypothesize about what impact the NIST Framework might have on shaping a cybersecurity duty of care not only in the United States but also in the EU and India.[30] It should also be noted that this represents merely an initial attempt to frame some of the many topics coming out of the NIST process. Follow-up studies will be required, especially after (and assuming) more firms have begun adopting the Framework, to assess the long-term impact of the NIST Framework on managing the global cyber threat.

I. REVIEW OF EXISTING U.S. LAW SHAPING A CYBERSECURITY DUTY OF CARE

What constitutes the burgeoning field of "cybersecurity law and policy" is open to debate—but likely encompasses a wide array of topics from cyber-crime and privacy to data protection, contracts, torts, intellectual property, and even Internet governance.[31] For the present purposes, cybersecurity refers to the policy field

---

Ensure a High Common Level of Network and Information Security across the Union, at 3, COM (2013) 48 final (Feb. 7, 2013) (requesting legislative measures to improve on the current, voluntary approach to cybersecurity standards of care).

29. Efforts to date aimed at defining "cyber peace" have been minimal. The International Telecommunication Union (ITU), a U.N. agency specializing in information and communication technologies (ICTs) has likened "cyber peace" as being a necessary element in a "universal order of cyberspace" built on a "wholesome state of tranquility, the absence of disorder or disturbance and violence." Henning Wegener, *Cyber Peace*, *in* THE QUEST FOR CYBER PEACE 77, 78 (2011), *available at* http://www.itu.int/dms_pub/itu-s/opb/gen/S-GEN-WFS.01-1-2011-PDF-E.pdf. Although certainly desirable, such an outcome is politically unlikely and technically infeasible. *See* Joseph S. Nye, Jr., *Power and National Security in Cyberspace*, *in* 2 AMERICA'S CYBER FUTURE: SECURITY AND PROSPERITY IN THE INFORMATION AGE 5, 19–20 (Kristin M. Lord & Travis Sharp eds., 2011) (stating that many countries disagree about the scope or extent of enforcement of a future cyber treaty); *but see* Scott Shackelford, *The Meaning of Cyber Peace*, 2 NDIAS Q. 12, 13 (2013), *available at* http://www3.nd.edu/~gosborn/NDIAS-Quarterly_Fall-2013/FLASH/index.html (arguing that "[i]nstead of focusing on a single path to cyber peace," which is untenable due to the divergent ideas of what cybersecurity requires, global cyber peace should follow a "polycentric framework").

30. These jurisdictions were chosen as case studies since they have to date relied on a voluntary approach to enhancing national and regional cybersecurity similar to the United States. Moreover, especially in the case of the European Union (EU), U.S.–EU policymakers are in regular contact and the NIST Framework could do much to shape EU efforts in this space. *See generally Official: EU Eying NIST Framework With 'Great Interest'*, INSIDE CYBERSECURITY (Feb. 4, 2014), http://insidecybersecurity.com/index.php?option=com_user&view=login&return=aHR0cDovL2luc2lkZWN5YmVyc2VjdXJpdHkuY29tL0N5YmVyLURhaWx5LU5ld3MvRGFpbHktTmV3cy9vZmZpY2lhbC1ldS1leWluZy1uaXN0LWZyYW1ld29yay13aXRoLWdyZWF0LWludGVyZXN0L21lbnUtaWQtMTA3NS5odG1s (discussing official EU interest in the NIST framework).

31. *See* FISCHER, *supra* note 21, at summary, para. 3 ("More than 50 statutes address various aspects

concerned with managing cyber threats, including unauthorized access, disruption, and modification of electronically stored information, software, hardware, services, and networks.[32] The cyber threat matrix itself is always evolving; it consists of activities ranging from cyber economic-espionage that targets trade secrets and is carried out by transnational criminal organizations—sometimes at the behest of nation states—to "hacktivists" out to make a political point.[33] Many firms have begun to proactively invest in cybersecurity best practices to better protect themselves against increasingly sophisticated attackers,[34] but the ever-changing nature of the problem and sheer number of actors involved have made crafting a cybersecurity standard of care difficult.

Yet despite gaps in the legal framework and the ever-changing cyber threat, courts are increasingly willing to hold both organizations and firms liable for not protecting sensitive information. For example, the Michigan Court of Appeals held a union responsible for failing to safeguard the private information of members who became victims of identity theft.[35] Additionally, a federal court judge in Michigan ruled that a local bank was at fault for not detecting earlier the losses its customers sustained through a phishing attack.[36]

There have also been major class actions filed in invasion of information privacy lawsuits. Two such cases filed in 2003 against several of the largest information brokers in the United States also implicated the state of Florida for not protecting the privacy of its residents.[37] Damages sought were more than $2500 per violation, adding up to billions under the federal Driver Privacy Protection Act.[38] Ultimately, one of the defendant banks in the case was fined $50 million for purchasing data containing the personal information of hundreds of thousands of Florida residents for just $5656.[39] In 2006, ChoicePoint, a large data broker that maintains digital dossiers on many adults in the United States, was fined $10 million by the Federal Trade Commission (FTC)—at that point "the largest civil penalty in the agency's history."[40]

---

of cybersecurity either directly or indirectly, but there is no overarching framework legislation in place.").

32. *See* 44 U.S.C. § 3542(b)(1) (2012) (defining "information security" as "protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction").

33. *E.g.*, Alex Stark, *Review—Cybersecurity and Cyberwar*, E-INTERNATIONAL REL. (Jan. 6, 2014), http://www.e-ir.info/2014/01/06/review-cybersecurity-and-cyberwar/ (reviewing P.W. Singer & Allan Friedman, CYBERSECURITY AND CYBERWAR: WHAT EVERYONE NEEDS TO KNOW (2014)).

34. *See generally* FIN. INDUS. REGULATORY AUTH., REPORT ON CYBERSECURITY PRACTICES (2015).

35. Bell v. Mich. Council 25 of the Am. Fed'n of State, Cnty., & Mun. Emps., No. 246684, 2005 WL 356306, at *5 (Mich. Ct. App. Feb. 15, 2005).

36. *ACH Liability Up for Grabs as Court Finds against Bank in Second US Cyber-Heist Suit*, FINEXTRA (June 17, 2011), http://www.finextra.com/news/fullstory.aspx?newsitemid=22674.

37. DAVID H. HOLTZMAN, PRIVACY LOST: HOW TECHNOLOGY IS ENDANGERING YOUR PRIVACY 112 (2006) (quoting Dan Christensen, *Major Information Brokers Face Class Action for Invasion of Privacy*, LAW.COM, June 24, 2003, http://www.law.com/jsp/article.jsp?id=1056139884864&slreturn=1 (on file with author)).

38. *Id.*; 18 U.S.C. § 2724(a) (2000).

39. K.C. Jones, *Bank to Pay $50 Million for Buying Personal Data*, INFORMATIONWEEK (Aug. 29, 2006), http://www.informationweek.com/bank-to-pay-50-million-for-buying-person/192500171.

40. Gary Rivlin, *Keeping Your Enemies Close*, N.Y. TIMES, Nov. 12, 2006, http://www.nytimes.com/2006/11/12/business/yourmoney/12choice.html?_r=1. Likewise, in a similar instance the personal information of more than 540,000 New Yorkers was compromised when sensitive computer hardware went missing from a supposedly secure facility. *See, e.g.*, *540,000 New Yorkers at Risk of Identity Theft*, NBC NEWS

In all, hundreds of millions of personal records have been exposed in thousands of incidents.[41] A single incident in 2006 involving the theft of a laptop owned by the Veterans Administration led to the loss of 26 million social security numbers of retired and active duty military personnel,[42] resulting in a class action lawsuit claiming more than $26.5 billion in damages.[43] Yet litigation is by no means universally successful. In late 2012, for example, a federal judge dismissed a case against Sony resulting from its massive data breach on the grounds that its users signed a privacy policy that contained "clear admonitory language that Sony's security was not 'perfect,'" and, therefore, "no reasonable consumer could have been deceived."[44]

Other courts have considered whether victims of identity theft may bring a claim against financial institutions that have carelessly handled their personal information, sometimes arriving at contradictory rulings.[45] Still other decisions have recognized a broad tort duty of confidentiality, which suggests that banks and other protectors of private information have a fundamental duty to keep their customers' personal information secure and confidential.[46] Some scholars are getting creative, advocating for an independent tort of "negligent enablement of cybercrime" based on principles of premises liability (requiring that landowners who open their land to the public must use reasonable care in ensuring safety for their guests), product liability (holding producers liable for defective products), and warranty.[47] Such a tort is meant to get around mass-market license agreements (the "accept" checkbox), which typically include liability waivers for negligent software design, and could help protect consumers against breaches caused by foreseeable software flaws, shifting the burden to the party best able to evaluate cybersecurity.[48] Other lawsuits have been

---

(July 24, 2006), http://www.msnbc.msn.com/id/14015598/ns/technology_and_science-security/t/new-yorker s-risk-identity. CS Stars, a Chicago-based insurance broker, was responsible for the system, which was ultimately recovered by the FBI. *Computer Holding Personal Data Found*, NBC NEWS (July 26, 2006), http://www.nbcnews.com/id/14047484/ns/technology_and_science-security/t/computer-holding-personal-data-found/#.VQ7r52TF_38.

41. *See, e.g.*, *Chronology of Data Breaches: Security Breaches 2005–Present*, PRIVACY RIGHTS CLEARINGHOUSE, http://www.privacyrights.org/data-breach (last updated Dec. 31, 2013) (chronicling record breaches, with a running total approaching one billion total breaches).

42. Joris Evers, *Veterans Affairs Faulted in Data Theft*, ZDNET (July 12, 2006), http://www.zdnet.com /news/veterans-affairs-faulted-in-data-theft/148782.

43. Cindy Waxer, *The Hidden Cost of IT Security*, NETWORK SECURITY J. (Apr. 16, 2006), http://www.networksecurityjournal.com/features/hidden-cost-of-IT-security-041607/ (discussing the rise of IT costs in an attempt to avoid increasingly high financial damages from security breaches).

44. *In re* Sony Gaming Networks & Customer Data Sec. Breach Litig., 903 F. Supp. 2d 942, 968 (S.D. Cal. 2012); *cf.* Schnall v. The Hertz Corp., 78 Cal. App. 4th 1144, 1163–69 (2000) (finding disclaimers do not give notice to the reasonable consumer when they are incomprehensible and needlessly complex).

45. *See, e.g.*, Brandon McKelvey, Comment, *Financial Institutions' Duty of Confidentiality to Keep Customer's Personal Information Secure from the Threat of Identity Theft*, 34 U.C. DAVIS L. REV. 1077, 1095–110 (2001) (describing consumers' reliance on causes of action against financial institutions for their failure to protect consumer information and indicating that courts do not universally recognize the causes of action).

46. *E.g.*, Peterson v. Idaho First Nat'l Bank, 367 P.2d 284, 290 (Idaho 1961) (holding that it is implicit in contracts between banks and consumers that banks have a duty to refrain from disclosing consumers' financial information).

47. *E.g.*, Michael L. Rustad & Thomas H. Koenig, *The Tort of Negligent Enablement of Cybercrime*, 20 BERKELEY TECH. L.J. 1553, 1607–10 (2005).

48. *See id.* at 1610–11 (suggesting that the tort of negligent enablement will protect software users by holding software producers, who currently waive their responsibility in "anti-warranty" licensing

brought under the theory of "negligent enablement of imposter fraud."[49] However, these have so far been unsuccessful because of an absence of the duty element required in a negligence suit.[50]

This Part builds from the foregoing discussion by assessing how common and statutory law are shaping a standard of cybersecurity care before considering what impact the NIST Framework might have on this regime. The Part begins by analyzing whether a standard of care might now be emerging in negligence cases. Then, it assesses the applicability of fiduciary duties. Finally, this Part considers some of the applicable statutory schemes related to critical infrastructure protection. Throughout, we argue that, at best, a cybersecurity standard of care in the U.S. context should be considered to be incomplete and immature, opening the door for the NIST Framework to have considerable impact on establishing such a standard.

A. Determining a Standard of Cybersecurity Care in Negligence Liability

Negligence, put simply, is conduct that "falls below the standard established by law for the protection of others against unreasonable risk of harm."[51] Avoiding liability for negligence generally requires conforming to a standard of conduct equivalent to that of another that would be considered "reasonable . . . under like circumstances."[52] A legislature or the courts may define this standard of conduct.[53] In all contexts, including cybersecurity, negligence might apply both to an action or omission—that is, failure to act when a duty was owed to do so.[54] In cybersecurity law, there is no explicit or overt "cybersecurity negligence" framework,[55] although attempts have been made to categorize cybersecurity negligence cases that highlight how each of the four negligence prongs have been met,[56] perhaps demonstrating that a standard may be slowly emerging.

The standard of care in negligence is not static but rather evolves over time along with technological advancements. A commonly utilized approach to determining negligence has been the "risk/utility formula" famously articulated by

---

agreements, responsible for damages caused by software failures).

49. *E.g.*, Huggins v. Citibank, N.A., 585 S.E.2d 275, 276 (S.C. 2003).

50. *E.g.*, *id.* at 277; *see also* Chris Jay Hoofnagle, *Putting Identity Theft on Ice: Freezing Credit Reports to Prevent Lending to Impostors*, *in* SECURING PRIVACY IN THE INTERNET AGE 207, 213–14 (Anupam Chander et al. eds., 2008) (describing the court's decision in *Huggins v. Citibank, N.A.*). Portions of this research first appeared in Scott J. Shackelford, *Should Your Firm Invest in Cyber Risk Insurance?*, 55 BUS. HORIZONS 349 (2012).

51. RESTATEMENT (SECOND) OF TORTS § 282 (1965).

52. *Id.* § 283.

53. *Id.* § 285.

54. *Id.* § 284.

55. *See supra* notes 22–28 and accompanying text.

56. *See* Picanso, *supra* note 23, at 376 (breaking down state-level cases by each negligence prong, examining findings of "liability for damages resulting from inadequate data security measures and obstacles to recovery"). These prongs include: duty of care and breach, *see, e.g.*, Bell v. Mich. Council 25 of the Am. Fed'n of State, Cnty., & Mun. Emps., No. 246684, 2005 WL 356306, at *1–2 (Mich. Ct. App. Feb. 15, 2005) (noting how to find the "special relationship" required to establish a duty); Remsberg v. Docusearch, Inc., 816 A.2d 1001, 1008 (N.H. 2003) ("[T]he risk of criminal misconduct is sufficiently foreseeable so that an investigator has a duty to exercise reasonable care in disclosing a third person's personal information to a client."), and causation and injury, *e.g.*, Stollenwerk v. Tri-West Healthcare Alliance, No. Civ. 03-0185PHXSRB, WL 2465906, at *5 (D. Ariz. Sept. 6, 2005).

Judge Learned Hand of the Second Circuit Court of Appeals.[57] Suggestions of the formula's use appeared in 1932, when a group of tugboats were hit by a storm and sank, resulting in the loss of its cargos of coal.[58] In the resulting lawsuit, the plaintiffs argued that the tug vessels were "unseaworthy" because they did not have radio receiving sets, which would have warned the tugboats of the storm and prevented the loss of the barges and cargo.[59] The tugboat companies defended themselves on the basis that they were following the prevailing standard practice of the industry: Radio receivers were expensive to purchase and maintain, so they were not typically found in tugboats. Therefore, the companies should not be liable.[60] However, Judge Learned Hand broke new ground, writing that even though having radios aboard was not yet an established industry custom, "[c]ourts must in the end say what is required; there are precautions so imperative that even their universal disregard will not excuse their omission."[61]

Judge Hand would be faced with a similar opportunity to articulate what should be required in *United States v. Carroll Towing Co.*[62] In this case, Judge Hand devised a formula for determining negligence, focusing on three primary elements: "(1) The probability that [injury will occur]; (2) the gravity of the resulting injury, if [it occurs]; and (3) the burden of adequate precautions."[63] Thus, "liability depends upon whether B [the burden of adequate precautions] is less than L [the gravity of the injury] multiplied by P [the probability of the harm]"—articulated in the algebraic formula $B < P*L$.[64] Though cybersecurity negligence case law is still in its infancy, a number of scholars have looked to Judge Hand's "risk/utility formula" as a means of determining liability for companies who suffer damage from lax cybersecurity.[65]

An open question extending from this case law, then, is whether judges should exercise similar discretion in requiring companies to better manage cyber attacks by boasting a given set of cybersecurity best practices. For example, firewalls and anti-virus software regularly rank as the security technologies most often used in cybersecurity surveys, but few companies regularly update such software.[66] After that, percentages drop off. Roughly 65% of companies used encryption for data in

57. *See, e.g.*, David G. Owen, *The Graying of Products Liability Law: Paths Taken and Untaken in the New* Restatement, 61 TENN. L. REV. 1241, 1251–52 (1994) (indicating that courts have often applied the risk-utility approach, which Learned Hand made famous, to determining negligence).

58. The T.J. Hooper (*In re* E. Transp. Co.) v. H. N. Hartwell & Son, Inc., 60 F.2d 737, 737 (2d Cir. 1932).

59. *Id.*

60. *Id.* at 740.

61. *Id.*

62. United States v. Carroll Towing Co., 159 F.2d 169 (2d Cir. 1947).

63. *Id.* at 173.

64. *Id.*

65. *E.g.*, Michael L. Rustad & Thomas H. Koenig, *Extending Learned Hand's Negligence Formula to Information Security Breaches*, 3 I/S J.L & POL'Y FOR INFO. SOC'Y 237, 244–53 (2007) [hereinafter Rustad & Koenig, *Extending Hand's Formula*] (explaining how Learned Hand's formula can be applied to cybersecurity); Robert Carolina, *The Reasonable Person in Cyber Security: When Did We Become Negligent?*, YOUTUBE (Feb. 24, 2014), http://www.youtube.com/watch?v=Di9aWQ4M8dk (explaining the reasonable person standard in cybersecurity).

66. *See, e.g.*, WADE BAKER ET AL., 2011 DATA BREACH INVESTIGATIONS REPORT 62–64 (2011), *available at* http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf (showing inconsistent rates of using and updating firewalls and anti-virus software).

transit according to 2011 surveys conducted by Computer Science Institute and Verizon.[67] About half use intrusion prevention systems and encryption for data in storage, while approximately one-third use public-key encryption, specialized wireless security systems, or content-monitoring systems to prevent data loss.[68] However, these fractions are constantly changing,[69] which raises questions: For example, would a judge be justified in finding a firm negligent that suffered a data breach due to firewalls or spyware that had not been updated, even if many companies do not regularly update? What about not encrypting data at rest and in transit, or failing to do regular penetration testing?

Though the risk/utility formula has yet to be fully analyzed by a court within a cybersecurity context, courts have addressed what constitutes reasonable standards of cybersecurity care through alternative rationales with varying outcomes. Some courts, for example, have looked to established practices to determine whether a trier of fact should be allowed to determine negligence; however, this approach is by no means consistent. Consider Sony, which in May 2011 was attacked with hackers reportedly compromising more than 100 million gamers' names, addresses, emails, user names, and passwords.[70]

In the ongoing case, *In re Sony Gaming Networks and Customer Data Security Breach Litigation*,[71] the court suggested that Sony's failure to employ industry cryptology standards was enough for plaintiffs to allege that Sony breached its duty to employ reasonable data security measures.[72] In their complaint, victims of the hack alleged that Sony had a duty "to design, implement, maintain, and test Sony's security system in order to ensure Plaintiffs' Personal Information was adequately secured and protected" and that "Sony breached this duty by failing to implement proper procedures to protect Plaintiffs' Personal Information."[73] Sony contested, arguing, among other things, that it had no legal duty to provide reasonable security.[74] Based on California and Massachusetts law,[75] the court in this case agreed with the plaintiffs, finding,

---

67. *Id.*

68. *Id.*

69. *See id.* at 63 (demonstrating the constantly changing number of companies using security technologies).

70. Ian Sherr & Amy Schatz, *Sony Deails Hacker Attack*, WALL ST. J., May 5, 2011, http://online.wsj.com/article/SB10001424052748703849204576302970153688918.html; Hayley Tsukayama, *Cyber Attack Was Large-Scale, Sony Says*, WASH. POST, May 4, 2011, http://www.washingtonpost.com/ blogs/faster-forward/post/cyber-attack-was-large-scale-sony-says/2011/05/04/AF78yDpF_blog.html; Nick Bilton, *Sony Explains PlayStation Attack to Congress*, N.Y. TIMES BITS BLOG (May 4, 2011), http://bits.blogs.nytimes.com/2011/05/04/sony-responds-to-lawmakers-citing-large-scale-cyberattack/.

71. *In re* Sony Gaming Networks and Consumer Data Sec. Breach Litig., 996 F. Supp. 2d 942 (S.D. Cal. 2014).

72. *Id.* at 966.

73. *Id.*

74. *Id.*

75. The complaint asserted negligence claims under California law, Florida law, Massachusetts law, Missouri law, and Ohio law. *Id.* at 963. The Florida, Missouri, and Ohio negligence claims' allegations of causation and harm, however, were "wholly conclusory, and therefore fail[ed] to put the Court or Sony on notice of the specific relief requested." *Id.* The court addressed the California and Massachusetts negligence claims separately.

> [B]ecause Plaintiffs allege that they provided their Personal Information to Sony as part of a commercial transaction, and that Sony failed to employ reasonable security measures to protect their Personal Information, including the utilization of industry-standard encryption, the Court finds Plaintiffs have sufficiently alleged a legal duty and a corresponding breach.[76]

Beyond particular technologies, other courts have placed considerable weight on industry report recommendations, which may be considered similar to the NIST Framework, in determining whether a reasonable level of data security had been provided by an entity.[77] For instance, in *Shames–Yeakel v. Citizens Financial Bank*, the U.S. District Court for the Northern District of Illinois found that Citizens' failure to comply with security measures recommended in a report by the Federal Financial Institutions Examination Council (FFIEC) was enough to establish a triable issue of fact as to whether Citizens breached its duty of care.[78] Marsha Shames–Yeakel was the owner of a bookkeeping company, "Best Practices," which had a business checking account with Citizens Financial Bank.[79] According to the court, an "unknown person" gained access to Shames–Yeakel's credentials, stealing upwards of $26,500 on Shames–Yeakel's home equity credit line.[80] Shames–Yeakel argued that Citizens' online banking security "lagged behind industry standards,"[81] as Citizens Financial Bank only used "single-factor identification" as opposed to "multifactor identification."[82] Specifically, Shames–Yeakel cited the FFIEC's Report, Authentication in an Internet Banking Environment,[83] which "does not endorse any particular technology" but states that "agencies consider single-factor authentication, as the only control mechanism, to be inadequate for high-risk transactions involving access to customer information or the movement of funds to other parties."[84] Citizens filed a motion for summary judgment, arguing, in part, that though it had a duty to protect its customer data, Shames–Yeakel had not produced sufficient evidence that Citizens had breached its duty of care.[85] The court denied Citizens' motion for summary judgment as to Shames–Yeakel's negligence claim.[86] While an expert retained by Citizens found the bank's use of single-factor

76. *Id.* *But see supra* note 44 and accompanying text.

77. *Cf.* Willingham v. Global Payment Inc., No. 1:12-CV-01157-RWS, 2013 WL 440702, at *19 (N.D. Ga. Feb. 5, 2013) (reflecting an alternative view in which courts are reluctant to rely on data security standards as a means of determining whether a duty was owed, let alone whether they should be used to determine reasonable standards of care).

78. 677 F. Supp. 2d 994, 1008–09 (N.D. Ill. 2009).

79. *Id.* at 997.

80. *Id.* at 998.

81. *Id.* at 1000.

82. *Id.* at 1000–01. Single-factor identification is the use of one authentication factor to satisfy validation (such as a "knowledge" factor like the use of a username and password). Multi-factor identification requires more than one authentication factor. *Cf. Azure Multi-factor Authentication*, MICROSOFT AZURE, http://azure.microsoft.com/en-us/services/multi-factor-authentication/ (last visited Mar. 23, 2015) (providing information on the benefits of multi-factor authentication services).

83. FED. FIN. INSTS. EXAMINATION COUNCIL, AUTHENTICATION IN AN INTERNET BANKING ENVIRONMENT (2005), *available at* http://www.ffiec.gov/pdf/authentication_guidance.pdf.

84. *Id.* at 1; *accord Shames–Yeakel*, 677 F. Supp. 2d at 1001.

85. *Shames–Yeakel*, 677 F. Supp. 2d at 1008.

86. *Id.* at 1009.

authentication to be "reasonable," the court stated that Citizens' "delay" in complying with FFIEC security standards could lead "a reasonable finder of fact [to] conclude that the bank breached its duty to protect Plaintiffs' account against fraudulent access."[87]

The lacking judicial analysis of what constitutes reasonable standards of cybersecurity care stems in part from the numerous barriers that exist to pursuing tort claims related to cyber attacks. For example, Article III standing has been problematic in many negligent data security cases, as establishing the required "injury-in-fact" and "causation" can prove difficult.[88] Additionally, data breaches that "merely" result in pure economic losses have also prevented negligence cases from proceeding.[89] This "economic loss doctrine" holds that plaintiffs must suffer physical damage (either to the person or the person's property) beyond mere economic losses in order to establish injury under negligence.[90] Because most injuries resulting from a lack of data security are purely economic—such as fraudulent charges on a user's account—defendants have successfully avoided negligence liability by using the economic loss doctrine.[91] These alternative defenses, in turn, have often prevented in-depth judicial analysis on the standard of care issue in cybersecurity negligence cases, leading to a consideration of alternative doctrines—including fiduciary duties.

B. A Note on Leveraging Fiduciary Duties to Enhance Corporate Cybersecurity

In addition to suits for negligence, corporate officers and directors also may have liability stemming from their fiduciary duties to shareholders in the aftermath of a cyber attack.[92] Historically, the two types of fiduciary duties that apply to

87. *Id.*

88. *See, e.g.*, Katz v. Pershing, LLC, 672 F.3d 64, 80 (1st Cir. 2012) (holding that plaintiff failed to state actual or impending injury under Article III "because she does not identify any incident in which her data has ever been accessed by an unauthorized person"); Reilly v. Ceridian Corp., 664 F.3d 38, 42, 44 (3d Cir. 2011) (finding no "actual or imminent" injury where "no identifiable taking occurred" and "all that [was] known [was] that a firewall was penetrated"). *But see, e.g.*, Krottner v. Starbucks Corp., 628 F.3d 1139, 1143 (9th Cir. 2010) (finding injury in fact under Article III "[b]ecause the plaintiffs had alleged an act that increased their risk of future harm" after theft of a laptop containing personal data).

89. *See, e.g.*, Annett Holdings, Inc. v. Kum & Go, L.C., 801 N.W.2d 499, 503 (Iowa 2011) ("As a general proposition, the economic loss rule bars recovery in negligence when the plaintiff has suffered only economic loss.").

90. Ralph C. Anzivino, *The Economic Loss Doctrine: Distinguishing Economic Loss from Non-Economic Loss*, 91 MARQ. L. REV. 1081, 1082 (2008).

91. *E.g.*, *In re* TJX Cos. Retail Sec. Breach Litig., 564 F.3d 489, 498–99 (1st Cir. 2009); *In Re* Michaels Stores Pin Pad Litig., 830 F. Supp. 2d 518, 530–31 (N.D. Ill. 2011) ("Notably, other courts dealing with data breach cases have also held that the economic loss doctrine bars the plaintiff's tort claim because the plaintiff has not suffered personal injury or property damage."). *But see* Lone Star Nat'l Bank, N.A. v. Heartland Payment Sys., Inc. 729 F.3d 421, 423–27 (5th Cir. 2013) (holding that the economic loss doctrine, under certain circumstances, did not bar plaintiff's negligence claim for allegedly unreasonable data security practices by defendant). However, in such situations, liability for purely economic losses may be sought under contract law. Anzivino, *supra* note 90, at 1081.

92. *See* Joseph P. McMenamin, *Pandemic Influenza: Is There a Corporate Duty to Prepare?*, 64 FOOD & DRUG L.J. 69, 85 (2009) ("Some courts considering derivative suits appear to be prepared in some instances to hold corporate directors to a simple negligence standard, which may expose directors to liability for failure to take reasonable, cost-effective steps to protect the company's interests.").

corporate officers and directors have been: (1) duty of loyalty; and (2) duty of care.[93] Directors have long enjoyed a great deal of discretion that immunizes them from many lawsuits alleging a breach of their fiduciary duties under a rule known as the "business judgment rule," which is a presumption that directors are acting in the best interests of the company.[94] However, this presumption has gradually become less of a silver bullet.[95] For example, some courts have extended the duty of care to encompass "a duty of oversight requiring directors and officers to act affirmatively to assure that adequate information and compliance systems are in place."[96] This puts the onus to make proactive investments in cybersecurity best practices squarely on directors that have perhaps grown accustomed to the benefits of immunity stemming from the business judgment rule.

Fiduciary duties thus may be relevant to managing cyber attacks and shaping a cybersecurity duty of care.[97] Related to the burgeoning duty of oversight, liability may be found on the basis of a lack of good faith under the duty of loyalty if "(a) the directors utterly failed to implement any reporting or information system or controls; or (b) having implemented such a system or controls, consciously failed to monitor or oversee its operations thus disabling themselves from being informed of risks or problems requiring their attention."[98] These standards speak to the importance of effective organization in managing the cyber threat. Yet many firms are still not making necessary organizational changes. When Sony was hacked in early 2011, it famously did not have a chief information security officer (CISO) or senior manager devoted wholly to information security.[99] It was not alone. In 2006, only 43% of respondents to a PricewaterhouseCoopers (PwC) survey said that they had a CISO or other similar security executive, though by 2009, that rate had increased to 85%.[100] This increase may in part be explained by the fact that companies with CISOs have been shown to save more than 20% on data breach costs over those that do not, according to one Symantec survey.[101]

---

93. Julian Velasco, *How Many Fiduciary Duties Are There in Corporate Law?*, 83 S. CAL. L. REV. 1231, 1232–33 (2010).

94. McMenamin, *supra* note 92, at 86–87.

95. *See id.* at 92 ("[E]xtensive factual analysis of corporate directors' business decisions suggest that courts may be growing increasingly willing to review in detail the substance, rather than merely the procedure, of business decisions. This change in application of the business judgment rule means that the overall defense may be weaker and more unpredictable than in the past." (footnote omitted)).

96. Bob Uda, *A Duty of Care in Cyberspace*, ICCTF (Mar. 3, 2011), http://www.icttf.org/blogs/927/42/a-duty-of-care-in-cyberspace (emphasis omitted).

97. *Cf.* J. Wylie Donald & Jennifer Black Strutt, *Cybersecurity: Moving Toward a Standard of Care for the Board*, BLOOMBERG L. (Nov. 4, 2013), http://about.bloomberglaw.com/practitioner-contributions/cybersecurity-moving-toward-a-standard-of-care-for-the-board/ (discussing how the fiduciary duties could affect board of directors in the cybersecurity context).

98. *In re* Citigroup Inc. S'holder Derivative Litig., 964 A.2d 106, 123 (Del. Ch. 2009) (quoting Stone *ex rel.* AmSouth Bancorporation v. Ritter, 911 A.2d 362, 370 (Del. 2006)).

99. Dave Aitel, *Top Hacker Disasters of 2011: Five Critical Lessons for Businesses*, FOX BUS. (Dec. 5, 2011), http://www.foxbusiness.com/economy/2011/12/05/top-hacker-disasters-2011-five-critical-lessons-for-businesses.

100. Ralph DeFrangesco, *Chief Information Security Officer: A New Spin on an Old Job*, IT BUS. EDGE (Nov. 2, 2009), http://www.itbusinessedge.com/cm/blogs/defrangesco/chief-information-security-officer-a-new-spin-on-an-old-job/?cs=37172.

101. PONEMON INST., 2010 ANNUAL STUDY: U.S. COST OF A DATA BREACH 32 (2011), *available at* http://www.fbiic.gov/public/2011/mar/2010_Annual_Study_Data_Breach.pdf.

Shareholder lawsuits against companies and their executives for lax security measures have started to make headlines as well. In December 2013, Target disclosed that it was aware that hackers had gained "unauthorized access" to customer payment card data.[102] Later estimates would suggest that the breach affected some 70 million Target customers, one of the largest data breaches of a retail store in history.[103] Following disclosure of the breach, at least two shareholders have filed shareholder derivate lawsuits, alleging, among other claims, breach of fiduciary duty against dozens of Target executives.[104] One of the shareholders complaints claims that "[i]n violation of its express promise to do so, and contrary to reasonable customer expectations, Target failed to take reasonable steps to maintain its customers' personal and financial information in a secure manner."[105]

Executives at the hotelier Wyndham Worldwide Corporation are also at the center of a shareholder derivative lawsuit. The lawsuit alleges that Russian-based hackers were able to gain unauthorized access to Wyndham's corporate databases on three separate occasions, stealing the consumer information of more than 600.000 customers.[106] Similar to the Target complaint, shareholders claim that the Wyndham executives failed to take reasonable steps to maintain their customers' personal and financial information.[107] However, a federal judge dismissed the lawsuit with prejudice in October 2014. It will be some time before we know if similarly situated derivative lawsuits based on cybersecurity incidents, such as the Target lawsuit, will result in a similar outcome. Yet, as with negligence, the role of common law fiduciary duties in shaping a standard of cybersecurity care should not be ignored. Neither should the role of cybersecurity statutes relevant to safeguarding critical infrastructure, the topic we turn to next.

C. U.S. Statutory Law and Regulatory Requirements for Critical Infrastructure Cybersecurity

In addition to leveraging common law—including negligence and fiduciary duties—to help establish a standard of cybersecurity care, numerous state and federal statutes are also applicable. It is beyond the scope of this Article, though, to review all of these statutory regimes. Numerous secondary sources have ably done

---

102. Press Release, Target Corp., Target Confirms Unauthorized Access to Payment Card Data in U.S. Stores (Dec. 19, 2013), http://pressroom.target.com/news/target-confirms-unauthorized-access-to-payment-card-data-in-u-s-stores.

103. *See* Jia Lynn Yang & Amrita Jayakumar, *Target Says Up to 70 Million More Customers Were Hit by December Data Breach*, WASH. POST., Jan. 10, 2014, http://www.washingtonpost.com/business/economy/target-says-70-million-customers-were-hit-by-dec-data-breach-more-than-first-reported/2014/01/10/0ada1026-79fe-11e3-8963-b4b654bcc9b2_story.html (describing the Target data breach as one of the worst ever).

104. Verified Shareholder Derivative Complaint, Collier v. Steinhafel (D. Minn. Jan. 29, 2014) (No. 0:2014cv00266), *available at* http://www.dandodiary.com/wp-content/uploads/sites/265/2014/02/targetsuit1.pdf; Verified Shareholder Derivative Complaint for Breach of Fiduciary Duty and Waste of Corporate Assets, Kulla v. Steinhafel (D. Minn. Jan. 21, 2014) (No. 0:14–cv–00203–SRN–JSM) [hereinafter Kulla], *available at* http://www.dandodiary.com/wp-content/uploads/sites/265/2014/02/firsttargetcomplaint.pdf.

105. Kulla, *supra* note 104, para. 3.

106. Verified Shareholder Derivative Complaint for Breach of Fiduciary Duty, Waste of Corporate Assets, and Unjust Enrichment, Palkon v. Holmes, para. 74, No. 2:14–cv–01234–SRC–CLW (D.N.J. May 2, 2014) (redacted copy), *available at* http://www.dandodiary.com/wp-content/uploads/sites/265/2014/05/palcon1.pdf.

107. *Id.* para. 3.

this already.[108] However, it is worth summarizing several of the most applicable statutes and regulations related to establishing and shaping a cybersecurity standard of care for critical infrastructure organizations. This Subpart does so by analyzing select statutory and regulatory requirements associated with the case studies of finance, chemical, healthcare, and energy, facilities. Subsequently, state data breach statutes and their reasonable data security requirements are also considered. As this Subpart demonstrates, rather than establishing explicit best practices, these legal requirements rely heavily on company implementation of broader reasonable and appropriate security measures.

1. Financial Sector: Gramm-Leach-Bliley Act Safeguard Rules

While its information practices are governed by a variety of statues, regulations, and best practices, the financial sector's most significant data security regulations derive in part from the Financial Services Modernization Act of 1999, also known as the Gramm-Leach-Bliley Act (GLBA).[109] The GLBA was enacted, in part, to provide "a prudential framework for the affiliation of banks, securities firms, . . . and other financial service providers."[110] Under the GLBA, "financial institutions"[111] are required to "protect the security and confidentiality of those customers' nonpublic personal information."[112] Specifically, authorized agencies are required to establish appropriate administrative, technical, and physical safeguards for financial institutions:

> (1) [T]o insure the security and confidentiality of customer records and information;
>
> (2) to protect against any anticipated threats or hazards to the security or integrity of such records; and
>
> (3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.[113]

Numerous agencies, including the FTC and the Securities and Exchange Commission (SEC), have since established certain rules and regulations to maintain

---

108. *E.g.*, FISCHER, *supra* note 21, at 52–61 (listing various federal laws identified as being related to cybersecurity).

109. Gramm-Leach-Bliley Act, Pub. L. No. 106–102, 113 Stat. 1338 (1999) (codified as amended in scattered sections of 12 and 15 U.S.C.).

110. *Id.* pmbl.

111. A "financial institution" is broadly defined as any institution that is engaging in activities that are financial in nature. *See* 15 U.S.C. § 6809(3)(A) (2012) ("The term 'financial institution' means any institution the business of which is engaging in financial activities as described in section 1843(k) of title 12."); 12 U.S.C. § 1843(k) (setting forth a number of activities which are financial in nature).

112. 15 U.S.C. § 6801(a); *see also* Guin v. Brazos Higher Educ. Serv., No. Civ. 05-668 RHK/JSM, 2006 WL 288483, at *3–4 (D. Minn. Feb. 7, 2006) (stating that "[i]n some negligence cases [] a duty of care may be established by statute," and applying the Gramm-Leach-Bliley Act (GLBA) to establish the duty of care, but holding that there was not a breach of that duty in the case).

113. 15 U.S.C. § 6801(b).

and enforce data security safeguards. For instance, the FTC's "Safeguard Rule" requires covered financial institutions to "develop, implement, and maintain a comprehensive information security program that ... contains administrative, technical, and physical safeguards that are appropriate to [an organization's] size and complexity, the nature and scope of [an organization's] activities, and the sensitivity of any customer information at issue."[114] This program must be "reasonably designed to achieve the objectives" of the GLBA.[115] The FTC Safeguard Rule additionally calls for the program to (1) designate an employee to coordinate the program; (2) "identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information"; (3) design safeguards to control the identified risks; (4) oversee financial service providers; and (5) provide continuous oversight for the program.[116] Financial entities under the authority of the SEC must follow similar safeguard standards. Under the SEC Safeguard Procedures, "[e]very broker, dealer, and investment company, and every investment adviser registered with the Commission" must adopt procedures "that address administrative, technical, and physical safeguards for the protection of customer records and information."[117]

2. Chemical Sector: Chemical Facility Anti-Terrorism Standards Regulation

In 2007, the U.S. Department of Homeland Security (DHS) promulgated the Final Rule of the Chemical Facility Anti-Terrorism Standards (CFATS).[118] These regulations are intended to "to enhance the security of our Nation by furthering the mission of the Department as provided in 6 U.S.C. §111(b)(1) and by lowering the risk posed by certain chemical facilities."[119] The CFATS requires certain high-risk chemical facilities to prepare "Security Vulnerability Assessment[s]" that "identify facility security vulnerabilities,"[120] and to implement "Site Security Plans" that

---

114. 16 C.F.R. § 314.3(a) (2014).

115. *Id.*

116. *Id.* § 314.4.

117. 17 C.F.R. § 248.30(a) (2009); *see also In re* J.P. Turner & Co., Exchange Act Release No. 3-13550, 98 SEC Docket 1729, 1741 (ALJ May 19, 2010) (initial decision) (ordering that J.P. Turner & Company cease committing violations of Rule 30(a)).

118. 6 C.F.R. § 27 (2007).

119. *Id.* § 27.100. "Chemical Facility" is defined within the Chemical Facility Anti-Terrorism Standards as

> any establishment that possesses or plans to possess, at any relevant point in time, a quantity of a chemical substance determined by the Secretary to be potentially dangerous or that meets other risk-related criteria identified by the Department. As used herein, the term chemical facility or facility shall also refer to the owner or operator of the chemical facility. Where multiple owners and/or operators function within a common infrastructure or within a single fenced area, the Assistant Secretary may determine that such owners and/or operators constitute a single chemical facility or multiple chemical facilities depending on the circumstances.

Id. § 27.105.

120. *Chemical Facility Anti-Terrorism Standards (CFATS)*, DEP'T HOMELAND SEC., http://www.dhs.gov/chemical-facility-anti-terrorism-standards (last updated Feb. 25, 2015); *accord* 6 C.F.R. § 27.215.

"include measures that satisfy the identified risk-based performance standards."[121] These Site Security Plans must include "appropriately risk-based measures," including efforts to "deter cyber sabotage, including by preventing unauthorized on-site or remote access to critical process controls, such as Supervisory Control and Data Acquisition (SCADA) systems."[122]

Guidance on the application of the CFATS standards are issued by the DHS Assistant Secretary, but "the acceptable layering of measures used to meet these standards will vary by risk-based tier."[123] The DHS, in an effort to assist high-risk facilities in meeting the CFATS requirements, published Risk-Based Performance Standards Guidance.[124] The publication provides examples of risk-based measures to satisfy the cyber standards; however, the publication "does not establish legally enforceable requirements for facilities subject to CFATS" and states that "the specific security measures and practices discussed in this document are neither mandatory nor necessarily the 'preferred solution'" for compliance.[125]

3. Healthcare and Public Health Sector: Health Insurance Portability and Accountability Act's Security Rules

The Health Insurance Portability and Accountability Act (HIPAA) was adopted in 1996,[126] tasking the federal government with, among other requirements, creating security standards to protect "individually identifiable health information" with which various health-care entities are responsible for complying.[127] More specifically, HIPAA authorized the Department of Health and Human Services to adopt "national standards that protect the confidentiality and integrity of electronic protected health information," or "ePHI."[128] These national standards, published in 2003, have been referred to as the "HIPAA Security Rule."[129] Under the Security Rule, covered entities "must assure their customers (for example, patients, insured individuals, providers, and health plans) that the integrity, confidentiality, and availability of electronic protected health information they collect, maintain, use, or transmit is protected."[130] HIPAA violations, including failing to comply with the standards or wrongfully disclosing personal information, may result in civil or

121. *Chemical Facility Anti-Terrorism Standards (CFATS)*, *supra* note 120.

122. 6 C.F.R. § 27.230(a)(8).

123. *Id.* § 27.230(a).

124. DEP'T OF HOMELAND SEC., RISK-BASED PERFORMANCE STANDARDS GUIDANCE: CHEMICAL FACILITY ANTI-TERRORISM STANDARDS (2009), *available at* http://www.dhs.gov/xlibrary/assets/chemsec_cfats_riskbased_performance_standards.pdf.

125. *Id.* at 7.

126. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat 1936 (codified as amended at scattered sections of 18, 26, 29, and 42 U.S.C.).

127. FISCHER, *supra* note 21, at 58.

128. Jennifer Griffin & David Elliott, *HIPAA Security Rule Compliance Reviews on the Horizon*, 76 DEF. COUNSEL J. 261, 262 (2009).

129. *The Security Rule*, DEP'T OF HEALTH & HUMAN SERV., www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/ (last visited Mar. 25, 2015).

130. Health Insurance Reform: Security Standards, 68 Fed. Reg. 8334, 8334 (Feb. 20, 2003). It should be noted that the Health Insurance Portability and Accountability Act (HIPAA) Security Rule does go into further detail about the cybersecurity requirements of covered entities than several other surveyed statutes.

criminal penalties;[131] the extent to which a private cause of action may exist under HIPAA is less clear.[132]

4. Energy Sector: North American Electric Reliability Corporation Standards

The North American Electric Reliability Corporation (NERC) is an international nonprofit regulatory body based in Atlanta, Georgia.[133] Under the Energy Policy Act of 2005, NERC is authorized to set mandatory standards in the operation of U.S. power systems, subject to financial penalties in the event of non-compliance.[134] The NERC "Reliability Standards" include nine critical infrastructure protection standards that mandate a variety of cybersecurity reporting, security identification, security implementation, and recovery requirements that are overseen by the Federal Energy Regulatory Commission (FERC).[135] The standards fit into a framework of protection, deterrence, prevention, limiting, and recovery.[136] Thus, in lieu of any actual overarching cybersecurity legislation, the authority given by Congress to the FERC stands in as a mechanism for creating mandatory cybersecurity standards in the critical infrastructure sphere.[137] The NERC also serves as a model of bottom-up governance in the form of industry best practices that were eventually sanctioned by the U.S. government after the 2003 northeast blackout.[138] Whether a similar pattern emerges regarding the NIST Framework remains to be seen.

5. State Data Security Regulations

In addition to federal regulatory requirements, state laws that call for "reasonable" security measures for certain types of personal information may also provide an opportunity for the NIST Framework to play a part in shaping what constitutes reasonable standards of cybersecurity care. Between 2002 and April

131. 42 U.S.C. § 1320d-5 (2012).

132. *See* Cory J. Fox, *HIPAA Violation Results in $1.44M Jury Verdict against Walgreens, Pharmacist*, BAKERHOSTETLER (Aug. 22, 2013), http://www.bakerlaw.com/health-law-update-august-22-2013#HIPAA ("Although HIPAA does not create a private cause of action, a recent Indiana Superior Court jury verdict demonstrates that HIPAA still could play an important role in private causes of action in state court based on negligence and professional liability . . . .").

133. *About NERC*, N. AM. ELECTRIC RELIABILITY CORP., http://www.nerc.com/AboutNERC/Pages/default.aspx (last visited Mar. 25, 2015).

134. *See* Roland L. Trope & Stephen J. Humes, *Before Rolling Blackouts Begin: Briefing Boards on Cyber Attacks that Target and Degrade the Grid*, 40 WM. MITCHELL L. REV 647, 665 n.33 (2014) (discussing NERC's authority to establish and enforce mandatory reliability standards).

135. *CIP Compliance*, N. AM. ELECTRIC RELIABILITY CORP., http://www.nerc.com/pa/CI/Comp/Pages/default.aspx (last visited Mar. 25, 2015).

136. *Critical Infrastructure Protection Committee (CIPC)*, N. AM. ELECTRIC RELIABILITY CORP., http://www.nerc.com/comm/CIPC/Pages/default.aspx (last visited Mar. 25, 2015).

137. *See* Trope & Humes, *supra* note 134, at 665 n.33 (discussing the authority and the role of the Federal Energy Regulation Commission (FERC)).

138. *See* INTELLIGENCE & NAT'L SEC. ALLIANCE, ADDRESSING CYBER SECURITY THROUGH PUBLIC-PRIVATE PARTNERSHIP: AN ANALYSIS OF EXISTING MODELS 7 (2009), *available at* http://www.insaonline.org/i/d/a/Resources/Addressing_Cyber_Security.aspx (describing the North American Electric Reliability Corporation origins as a voluntary standards setter that eventually was adopted by the FERC).

2014, 47 States passed data breach notification requirements, in some instances mandating government or private sector entities to provide notice to those whose "personally identifiable information" is lost.[139] Variations among States create a complex and sometimes contradictory regulatory environment for firms operating across jurisdictions;[140] for example, a handful of states have a "no-harm threshold law," meaning that it does not matter whether lost information was used in a way that harmed consumers or not—the mere fact that there has been a breach requires that notification be given.[141] States also have more-or-less-inclusive lists of personally identifiable information that must be lost for a breach to warrant disclosure.[142] Meanwhile, in the states that do not have any data breach notification laws as of 2014—Alabama, South Dakota, and New Mexico[143]—a company could knowingly have its customers' social security numbers breached but not inform those customers and still be legally compliant under state law.[144] The Obama Administration's mid-2009 Cyberspace Review laid out some proposals to address this issue.[145]

In addition to mandating requirements on entities responding to a data breach, many of these statutes include explicit requirements that covered entities holding certain types of sensitive information are required to implement and maintain "reasonable" security measures.[146] As with state data breach notification requirements, some state data security requirements are much more comprehensive than others. Massachusetts, considered to have one of the most wide-ranging state data security laws, not only requires organizations storing personal information of Massachusetts residents to have a written security plan to secure personal data, but also necessitates that the plan be regularly audited.[147] Others state statutes are more

139. *Security Breach Notification Laws*, NAT'L CONF. STATE LEGISLATURES (Jan. 12, 2015), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

140. *See id.* (listing the different breach notifications laws); *see also* Kevin J. O'Brien, *Europe Weighs Requiring Firms to Disclose Data Breaches*, N.Y. TIMES, Jan. 16, 2013, http://www.nytimes.com/2013/01/17/technology/17iht-data17.html (reporting that a proposed EU directive would require EU-wide data breach reporting for all firms that "run large databases, those used for Internet searches, social networks, e-commerce or cloud services").

141. Mike Tsikoudakis, *Patchwork of Data Breach Notification Laws Poses Challenge*, BUS. INS. (June 5, 2011), http://www.businessinsurance.com/apps/pbcs.dll/article?AID=/20110605/ISSUE03/306059998.

142. *See id.* (describing generally the types of state notification laws).

143. *Security Breach Notification Laws*, *supra* note 139.

144. *See* Jacqueline May Tom, *A Simple Compromise: The Need for a Federal Data Breach Notification Law*, 84 ST. JOHN'S L. REV. 1569, 1569–70 (2010) (discussing the effect of breach law on a state's duties).

145. *See* WHITE HOUSE OFFICE OF THE PRESS SEC'Y, CYBERSPACE POLICY REVIEW: ASSURING A TRUSTED AND RESILIENT INFORMATION AND COMMUNICATIONS INFRASTRUCTURE vi (2009), *available at* http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf [hereinafter CYBERSPACE POLICY REVIEW] (listing ten summary points of a near-term action plan for reforms in U.S. cybersecurity policies).

146. *E.g.*, ARK. CODE ANN. § 4-110-104(b) (2011); CAL. CIV. CODE § 1798.81.5(b) (West Supp. 2015); MD. CODE ANN. COM. LAW § 14-3503(a) (LexisNexis 2013); NEV. REV. STAT. § 603A.210.1 (2013); OR. REV. STAT. § 646A.622(1) (2013); R.I. GEN. LAWS § 11-49.2-2(2) (West 2013); TEX. BUS. & COM. CODE ANN. § 521.052 (West 2015).

147. Bart Lazar, *States Ramp Up Data Security Laws*, PCWORLD (Nov. 9, 2008), http://www.pcworld.com/article/153553/data_security-law.html.

general and do not specifically define what constitutes "reasonable" cybersecurity under the law.[148]

D. Summary

This Part has examined various existing and developing cybersecurity standards and frameworks under common and statutory law at the state and federal levels. As has been shown, there is not yet a comprehensive cybersecurity standard of care crystallizing across sectors, but we do see the beginnings of one with regards to negligence, the duty of oversight, and various statutory schemes to protect critical infrastructure. The situation is ripe for clarification. Whether the NIST Framework is an appropriate vehicle for addressing existing regulatory ambiguity is the subject we turn to next—after introducing its recent evolution and scope.[149]

II. INTRODUCING AND EXAMINING THE NIST CYBERSECURITY FRAMEWORK

Prior to President Obama's 2013 State of the Union Address and Executive Order 13636, efforts to update the regulatory provisions addressing critical infrastructure insecurity had largely stalled. In 2011, for instance, the Obama Administration released for consideration a comprehensive cybersecurity legislative proposal that intended to improve critical infrastructure protection.[150] Portions of the Administration's 2011 proposal had been introduced in both the House and the Senate,[151] but largely to no avail.[152] The Cybersecurity Act of 2012 would have tasked a new National Cybersecurity Counsel to work with private sector critical infrastructure owners and operators to identify critical cyber infrastructure, conduct sector-by-sector cyber risk assessments, and establish a voluntary, outcome-based cybersecurity program for critical infrastructure.[153] However, the bill faced

148. *See* John Black, *Developments in Data Security Breach Liability*, 69 BUS. LAW 199, 206 (2013) ("Although several states have data security laws that require businesses to adopt reasonable security measures to protect personal information . . . those statutes do not define what constitutes reasonable data security."); *see also* Johnson, *Data Security*, *supra* note 23, at 22 (stating that the California Security Breach Information Act "leaves no doubt that businesses owe a duty under California law to protect customers' personal information and that customers may recover damages if businesses breach that duty," yet "makes no attempt to define what constitutes 'reasonable security procedures and practices'").

149. *See* SHACKELFORD, MANAGING CYBER ATTACKS, *supra* note 3, at 244–45 (noting firms' concerns with regulatory intervention in cybersecurity).

150. Letter from Jacob J. Lew, Dir., Office of Mgmt. & Budget, to John Boehner, Speaker, U.S. House of Representatives (May 12, 2011), *available at* http://www.whitehouse.gov/sites/default/files/omb/legislative/ letters/Cybersecurity-letters-to-congress-house-signed.pdf ("The proposal would improve critical infrastructure protection by bolstering public-private partnerships with improved authority for the Federal government to provide voluntary assistance to companies and increase information sharing."); *see also* OFFICE OF MGMT. & BUDGET, EXEC. OFFICE OF THE PRESIDENT, LEGISLATIVE LANGUAGE: LAW ENFORCEMENT PROVISION RELATED TO COMPUTER SECURITY (2011), *available at* http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/law-enforcement-provisions-related-to-computer-security-full-bill.pdf (detailing the legislative language proposed by the Office of Management and Budget to the U.S. Congress).

151. FISCHER, *supra* note 21, at 5.

152. *See, e.g.*, *U.S. Senators Push Ahead with Cyber Security Legislation*, *supra* note 8 ("[S]pats over liability and privacy protections have thwarted passage of comprehensive cyber security bills thus far.").

153. Cybersecurity Act of 2012, S. 3414, 112th Cong. § 101 (2012). Senate Bill 3414 is not to be

opposition from the private sector[154] and failed to pass the Senate.[155] The recommendations issued by the House of Representatives House Republicans Cybersecurity Task Force[156] have also failed to result in legislation as of March 2015.[157] This legislative inertia prompted executive action by the Obama Administration.

A. Executive Order 13636 and the Objectives of the NIST Framework

Executive Order 13636, effective in February 2013, intended to balance effective critical infrastructure security measures with the maintenance of a cyber-environment that encourages efficiency, innovation, and economic prosperity.[158] The major directives of the Order included enhancing the scope and efficiency of cybersecurity information sharing programs,[159] assessing and coordinating privacy and civil liberties protections in cybersecurity activities,[160] and implementing a baseline framework and voluntary program to reduce cyber risk to critical infrastructure.[161] The Order itself provided a number of overarching objectives for the Cybersecurity Framework to fulfill. For example, it placed the Director of NIST in charge of developing a voluntary Framework that "include[s] a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks."[162] The Framework would use cybersecurity best practices, at both a national and international level, in order to provide a "prioritized, flexible, repeatable, performance-based, and cost-effective approach" that could help critical infrastructure manage cybersecurity risks.[163] The Framework's creators were tasked with developing an approach that could adapt well to future, unknown technologies while also allowing the Framework to be used

---

confused with Senate Bill 2105, an earlier bill of the same name, which would have tasked the Department of Homeland Security to identify "covered critical infrastructures" sectors and require owners of covered entities to remediate or mitigate identified cyber risks. Cybersecurity Act of 2012, S. 2105, 112th Cong. §§ 101–104 (2012).

154. *See, e.g.*, Letter from R. Bruce Josten, Exec. Vice President of Gov't Affairs, Chamber of Commerce, to the Members of the U.S. Senate (July 30, 2012), http://www.uschamber.com/ letter/key-vote-letter-s-3414-cybersecurity-act-2012%E2%80%9D (expressing that "[t]he [U.S. Chamber of Commerce] strongly opposes S. 3414").

155. Eric Engleman, *Cybersecurtity Bill Killed, Paving Way for Executive Order*, BLOOMBERG (Nov. 15, 2012), http://www.bloomberg.com/news/articles/2012-11-15/cybersecurity-bill-killed-paving-way-for-executive-order.

156. *See* HOUSE REPUBLICAN CYBERSECURITY TASK FORCE, 113TH CONG., RECOMMENDATIONS OF THE HOUSE REPUBLICAN CYBERSECURITY TASK FORCE 5 (2011) (providing recommendations on "how House Republicans should approach four issue areas within cybersecurity").

157. However, as of this writing there is movement on various cybersecurity measures hastened by major data breaches, such as Anthem. *See* Andy Greenberg, *Privacy Critics Go 0-2 with Congress Cybersecurity Bills*, WIRED (Mar. 26, 2015), http://www.wired.com/2015/03/privacy-critics-go-0-2-congress-cybersecurity-bills/ (reporting on the most recent bills in the House and Senate, which are expected to reach a vote on each floor by late April).

158. Exec. Order No. 13636, 78 Fed. Reg. 11739, 11739 (Feb. 12, 2013).

159. *Id.* at 11739–40.

160. *Id.* at 11740.

161. *Id.* at 11740–42.

162. *Id.* at 11741.

163. *Id.*

across industries.[164] The Framework was also intended to mature over time, allowing areas of improvement to be recognized and accounted for in future Framework variations.[165]

Privacy and civil liberties protections are also specifically emphasized within the Framework. The Order called for the Cybersecurity Framework and its associated information security measures to identify, assess, and mitigate the impact that security practices within the Framework may have on business confidentiality, individual privacy, and civil liberties.[166] It also requested agencies to coordinate and ensure that privacy and civil liberties protections are incorporated into all activities mandated by the Order generally. Specifically, "[P]rotections shall be based upon the Fair Information Practice Principles and other privacy and civil liberties policies, principles, and frameworks as they apply to each agency's activities."[167]

Executive Order 13636 provided NIST one year to develop the Cybersecurity Framework.[168] To help with this process, NIST held five framework workshops throughout 2013, bringing together a large and diverse contingent of stakeholders, including academics, government officials, and private sector industry members.[169] Meetings were held, webinars were presented, and informal sessions were scheduled to provide feedback throughout the course of the Framework's development.[170]

These efforts resulted in the release of a preliminary draft of the Framework on October 22, 2013,[171] just prior to the fifth workshop, which was held in November 2013.[172] The preliminary Framework would undergo relatively few adjustments before it was released in its final version in early 2014.[173] Among the more significant

---

164. *See* Exec. Order No. 13636, 78 Fed. Reg. at 11741 ("The Cybersecurity Framework shall focus on identifying cross-sector security standards and guidelines applicable to critical infrastructure. The Cybersecurity Framework will also identify areas for improvement that should be addressed through future collaboration with particular sectors and standards-developing organizations.").

165. *Id.*

166. *Id.*

167. *Id.* For an understanding of the Fair Information Practice Principles, see generally ROBERT GELLMAN, FAIR INFORMATION PRACTICES: A BASIC HISTORY VERSION 2.13 (2015), *available at* http://www.bobgellman.com/rg-docs/rg-FIPShistory.pdf.

168. Exec. Order No. 13636, 78 Fed. Reg. at 11741.

169. For workshop recordings and slides, see *Cybersecurity Framework—Workshops and Events*, NIST, http://www.nist.gov/cyberframework/cybersecurity-framework-events.cfm (last visited Mar. 31, 2015).

170. For the materials and resources that were produced and circulated throughout the creation of the NIST Cybersecurity Framework, see *Cybersecurity Framework—Archived Documents*, NIST, http://www.nist.gov/cyberframework/cybersecurity-framework-archived-documents.cfm (last updated Feb. 12, 2014).

171. NAT'L INST. OF STANDARDS & TECH., IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY EXECUTIVE ORDER 13636: PRELIMINARY CYBERSECURITY FRAMEWORK (2013), *available at* http://www.nist.gov/itl/upload/preliminary-cybersecurity-framework.pdf [hereinafter NIST PRELIMINARY CYBERSECURITY FRAMEWORK]; Press Release, NIST Releases Preliminary Cybersecurity Framework, Will Seek Comments (Oct. 22, 2013), http://www.nist.gov/itl/cybersecurity-102213.cfm.

172. *Cybersecurity Framework—Workshops and Events*, *supra* note 169.

173. Some of the minor adjustments included amending the Framework Core. For example, some of the Subcategories found in the "Identify" Function's "Risk Assessment" Category were restructured and included additional Informative References. *Compare* NIST CYBERSECURITY FRAMEWORK, *supra* note 2, at 22 ("ID.RA-3: Threats, both internal and external, are identified and documented."), *with* NIST PRELIMINARY CYBERSECURITY FRAMEWORK, *supra* note 171, at 15–16 ("ID.RA-3: Threats to organizational assets are identified and documented.").

revisions was the removal of verbiage designed to signal whether an organization has successfully implemented the Framework, stressing the "voluntary" nature of the Framework.[174] Certain terms, such as "adoption," were removed,[175] and greater emphasis was placed on the Framework's focus on critical infrastructure.[176] The most significant change came from the removal of the preliminary Framework's "Privacy Methodology," a detailed approach designed to address privacy and civil liberties considerations surrounding the deployment of cybersecurity activities.[177] Reflecting a concern among stakeholders that "the methodology did not reflect consensus private sector practices and therefore might limit use of the Framework,"[178] NIST incorporated an alternative privacy methodology developed by Hogan Lovells's partner Harriet Pearson.[179] The new privacy methodology, contained within the final version of the Framework, removes the organizational chart that would have corresponded to the Framework Core and instead provides a "general set of considerations and processes since privacy and civil liberties implications may differ by sector or over time and organizations may address these considerations and processes with a range of technical implementations."[180] Overall, the preliminary Framework provided the foundation for what would become version 1.0 of the final Framework.

B. Breakdown of the NIST Cybersecurity Framework

The Cybersecurity Framework takes a risk-based approach for organizations to detect, mitigate, and respond to cyber threats.[181] Rather than developing new

---

174. *See* NAT'L INST. OF STANDARDS & TECH, UPDATE ON THE DEVELOPMENT OF THE CYBERSECURITY FRAMEWORK 2 (2014) [hereinafter DEVELOPMENT OF THE CYBERSECURITY FRAMEWORK], *available at* http://www.nist.gov/cyberframework/upload/NIST-Cybersecurity-Framework-Update-011514-2.pdf ("A significant number of commenters stated that the Framework should reinforce throughout the document that it is intended to be voluntary.").

175. *See id.* ("While many commenters suggested incorporating the definition of 'adoption' previously identified by NIST, this was not an area of consensus as alternative definitions were proposed, and several commenters preferred that detail around adoption be reflected in use of the Framework or in supporting material.").

176. *See id.* ("NIST received comments recommending that the Framework state clearly that its focus is on the nation's critical infrastructure, while acknowledging that the document has broader utility and can be helpful to many parts of the economy.").

177. NIST PRELIMINARY CYBERSECURITY FRAMEWORK, *supra* note 171, at 28–35.

178. DEVELOPMENT OF THE CYBERSECURITY FRAMEWORK, *supra* note 174.

179. Letter from Harriet Pearson, Partner, Hogan Lovells, to Adam Sedgewick, Nat'l Inst. of Standards & Tech. (Dec. 5, 2013), http://csrc.nist.gov/cyberframework/framework_comments/20131205_harriet_pearson_hoganlovells.pdf.

180. NIST CYBERSECURITY FRAMEWORK, *supra* note 2, at 15.

181. Risk assessment and management is a complex process that has developed into its own, distinct area of expertise. "Risk," generally, refers to the "effect of uncertainty on objectives." International Organization for Standardization, *ISO 31000 2009: Plain English Introduction,* PRAXIOM RESEARCH GRP. LTD., http://www.praxiom.com/iso-31000-intro.htm (last visited Apr. 22, 2015). As the International Organization for Standardization's has further described:

> Whenever you try to achieve an objective, there's always the chance that things will not go according to plan. There's always the chance that you will not achieve what you expect to achieve. Every step you take to achieve an objective involves uncertainty. Every step has an

cybersecurity standards and risk management processes, the Cybersecurity Framework "relies on a variety of existing standards, guidelines, and practices to enable critical infrastructure providers to achieve resilience," which allows the Framework to "scale across borders, acknowledge the global nature of cybersecurity risks, and evolve with technological advances and business requirements."[182] The Cybersecurity Framework provides a "common language" for entities to evaluate their current cybersecurity posture, determine their targeted state for cybersecurity, prioritize opportunities for improvement, assess progress toward their targeted state, and establish sufficient methods of communication among internal and external stakeholders about cybersecurity risk.[183] The substance of the Cybersecurity Framework is composed of three parts: (1) The Framework Core, (2) The Framework Implementation Tiers, and (3) The Framework Profile. We investigate each element in turn.

1. Framework Core

The Cybersecurity Framework begins by laying out the Framework Core, which "provides a set of activities to achieve specific cybersecurity outcomes, and references examples of guidance to achieve those outcomes."[184] Neither an exhaustive list nor a checklist, the Framework Core is an organizational map of industry-recognized cybersecurity practices that are helpful in managing cybersecurity risk, and it provides unified terminology for organizations to understand successful cybersecurity practice outcomes.[185] The Framework Core is broken down into four elements—Functions, Categories, Subcategories, and Informative References—that assist in mapping applicable cybersecurity standards, guidelines, and best practices.[186]

The Core begins by delineating essential cybersecurity activities "at their highest level," referred to as Functions.[187] The Framework recognizes five Functions—Identify, Protect, Detect, Respond, and Recover[188]—that are intended to

---

> element of risk that needs to be managed . . . . [R]isk is the chance that there will be a positive or negative deviation from the objectives you expect to achieve.

Id. The process of identifying, assessing, and responding to risk is referred to as "risk management," and while the Framework itself is not a risk management process, it "uses risk management processes to enable organizations to inform and prioritize decisions regarding cybersecurity." NIST CYBERSECURITY FRAMEWORK, *supra* note 2, at 5.

182. NIST CYBERSECURITY FRAMEWORK, *supra* note 2, at 4.

183. *Id.* at 1.

184. *Id.* at 7.

185. *See id.* ("The Core is not a checklist of actions to perform. It presents key cybersecurity outcomes identified by industry as helpful in managing cybersecurity risk.").

186. *Id.* at 7–8. For a complete list of the applicable cybersecurity standards, guidelines, and best practices in the Framework Core, see *id.* app. A.

187. *Id.* at 7.

188. These Framework Core Functions are defined as follows:

> Identify-Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.. . . .
>
> Protect-Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.. . . .

assist an organization in expressing its management of cybersecurity risk by organizing practices into these key areas.[189] Each Function contains more detailed subsets of overarching practices, referred to as Categories, which are "groups of cybersecurity outcomes, closely tied to programmatic needs and particular activities."[190] Each Category assists an organization's approach to mapping the key Functions underlying the Cybersecurity Framework.[191] Each Category provides a brief description to more efficiently place it within the context of its corresponding Function, as well as to guide further categorization within the remaining Core elements. For example, the "Identify" Function contains within it the "Asset Management" Category, which articulates practice outcomes to identify and manage the "data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes . . . consistent with their relative importance to business objectives and the organization's risk strategy."[192]

> Detect-Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event. . . .
>
> Respond-Develop and implement the appropriate activities to take action regarding a detected cybersecurity event. . . .
>
> Recover—Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

NIST CYBERSECURITY FRAMEWORK, *supra* note 2, at 8–9.

189. *See id.* (explaining the categories within each Function and how they address cybersecurity risk).

190. *Id.* at 7.

191. *Cf. id.* app A at 19, tbl. 1 (listing Category Unique Identifiers for each Function).

192. *Id.* app. A at 20, tbl. 2.

Function	Category	Subcategory	Informative References
IDENTIFY (ID)	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	ID.AM-1: Physical devices and systems within the organization are inventoried	CCS CSC 1 COBIT 5 BAI09.01, BAI09.02 ISA 62443-2-1:2009 4.2.3.4 ISA 62443-3-3:2013 SR 7.8 ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 NIST SP 800-53 Rev. 4 CM-8

Fig. 1: NIST Framework Core Example[193]

Further subdividing the Framework Core are "specific outcomes of technical and/or management activities" referred to within the Framework as Subcategories.[194] These subcategories provide further detail for organizations to address each overarching Category. Building off of our previous example, one Subcategory of the "Identify" Function's "Asset Management" Category is the practice of keeping inventory of all organization devices and systems, articulated in the above example as ID.AM-1.[195] Each of these Subcategories receives a reference to the corresponding "standards, guidelines, and practices common among critical infrastructure sectors" that would provide methods for accomplishing the stated Subcategory practice, referred to as "Informative Reference[s]."[196] An organization, for example, looking for an established standard or guideline for device inventory related to federal systems and organizations could look to the Framework's suggested NIST Special Publication 800-53.[197] Specifically, the Framework directs an entity to the publication's "Configuration Management-8: Information System Component Inventory" within the publication's security controls.[198] It is within this document that an organization can review the specific control requirements, supplemental guidance to the control, and stated "control enhancements."[199] The Framework's Informative References are not intended to be an exhaustive list, and companies are

193. *Id.* at 8.

194. NIST CYBERSECURITY FRAMEWORK, *supra* note 2, at 8.

195. *See supra* fig.1; *see also* NIST CYBERSECURITY FRAMEWORK, *supra* note 2, app. A at 20 tbl.2 ("Physical devices and systems within the organization are inventoried").

196. NIST CYBERSECURITY FRAMEWORK, *supra* note 2, app. B at 38.

197. NAT'L INST. OF STANDARDS & TECH., U.S. DEP'T OF COMMERCE, NIST SPECIAL PUB. 800-53, SECURITY AND PRIVACY CONTROLS FOR FEDERAL INFORMATION SYSTEMS AND ORGANIZATIONS (2013), *available at* http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.

198. *See id.* app. F-CM at F-73 to 75 (stating that an organization satisfies this control if the organization, among other requirements, "[d]evelops and documents an inventory of information system components that . . . [a]ccurately reflects the current information system . . . [i]ncludes all components within the authorization boundary of the information system . . . [i]s at the level of granularity deemed necessary for tracking and reporting; and . . . [r]eviews and updates the information system component inventory").

199. *Id.*

encouraged to continue to identify new or revised standards, guidelines, or practices as the cybersecurity landscape evolves.[200]

2. The Framework Implementation Tiers

After mapping common cybersecurity activities and the various standards and practices employed to conduct these activities, the Framework provides a method for an organization to understand the degree to which its cybersecurity risk management practices match the characteristics described within the Framework, known as the Framework Implementation Tiers.[201] The Tiers provide a measurement for how organizations view and manage cybersecurity risk, taking into consideration an organization's current practices, the cyber threat environment, legal and regulatory requirements, business objectives, and organizational constraints, among other considerations.[202] Based upon an organization's evaluation of its practices, the organization can identify to which Tier it belongs. The Implementation Tiers consist of a range of four Tiers: Partial, Risk Informed, Repeatable, and Adaptive.[203]

Each Tier definition is broken down into three general subsections: (1) Risk Management Process; (2) Integrated Risk Management Program; and (3) External Participation.[204] These subsection definitions assist an organization in selecting its appropriate Tier.[205] The Risk Management Process subsection addresses the extent to which an organization's cybersecurity risk management practices are formalized, the breadth of these formalized practices, and the extent to which the practices actively adjust to the changing cybersecurity landscape.[206] The Integrated Risk Management Program subsection evaluates the level of awareness that managers and employees have of an organization's risk management practices, the level of involvement that managers and employees have in mitigating cybersecurity risks, and the level of cybersecurity information sharing that occurs within the organization.[207] Finally, the External Participation subsection evaluates the extent to which

---

200. The Privacy Methodology found within the NIST Cybersecurity Framework plays a role within the Framework Core as well. The Methodology calls on organizations, as they assess the Framework Core outlined in Appendix A of the Cybersecurity Framework, to consider a number of processes and activities that may be considered to address privacy and civil liberties implications. NIST CYBERSECURITY FRAMEWORK, *supra* note 2, at 16–17. The categories of these processes and activities include: "Governance of cybersecurity risk"; "Approaches to identifying and authorizing individuals to access organizational assets and systems"; "Awareness and training measures"; "Anomalous activity detection and system and assets monitoring"; and "Response activities, including information sharing or other mitigation efforts." *Id.*

201. *Id.* at 5.

202. *Id.* at 9. It is important to note that the "Tiers do not represent maturity levels," but that advancing to a higher tier "is encouraged when such a change would reduce cybersecurity risk and be cost effective." *Id.*

203. *Id.* at 10–11.

204. *Id.*

205. *See id.* ("Tiers . . . provide context on how an organization views cybersecurity risk and the processes in place to manage that risk. [Tiers] . . . describe an increasing degree of rigor and sophistication in cybersecurity risk management practices . . . .").

206. NIST CYBERSECURITY FRAMEWORK, *supra* note 2, at 10–11 (describing each of these factors for each Tier).

207. *Id.*

organizations coordinate and collaborate with other external entities to share threat information.[208]

3. The Framework Profile

While the Framework's Implementation Tiers gauge the degree and sophistication of an organization's overall cybersecurity risk management practices, the Framework Profiles are meant to align the particular Framework Core Functions, Categories, and Subcategories with an organization's own implementation scenarios.[209] For example, an organization could create a "Current Profile" that would indicate "the cybersecurity outcomes that are currently being achieved" and a "Target Profile" that would specify "the outcomes needed to achieve the desired cybersecurity risk management goals."[210] Comparing these Profiles would allow an organization to reveal "gaps" that should be addressed to meet the organization's cybersecurity risk management objectives and assist the organization in establishing a roadmap for achieving its Target Profile.[211] Overall, the drafters expressed that "successful implementation" of the Framework is based on an organization's ability to achieve its Targeted Profiles.[212]

208. *Id.*

209. *Id.* at 5.

210. *Id.* at 11.

211. *Id.* (stating that that the Target Profiles should be "well aligned with organizational and sector goals, consider[] legal/regulatory requirements and industry best practices, and reflect[] risk management priorities").

212. NIST CYBERSECURITY FRAMEWORK, *supra* note 2, at 9 ("Successful implementation of the Framework is based upon achievement of the outcomes described in the organization's Target Profile(s).").

	Risk Management Process	Integrated Program	External Participation
Tier 1: Partial	Organizational cybersecurity risk management practices are not formalized, and risk is managed in an *ad hoc* and sometimes reactive manner. Prioritization of cybersecurity activities may not be directly informed by organizational risk objectives, the threat environment, or business/ mission requirements.	There is limited awareness of cybersecurity risk at the organizational level and an organization-wide approach to managing cybersecurity risk has not been established. The organization implements cybersecurity risk management on an irregular, case-by-case basis due to varied experience or information gained from outside sources. The organization may not have processes that enable cybersecurity information to be shared within the organization.	An organization may not have the processes in place to participate in coordination or collaboration with other entities.
Tier 2: Risk-Informed	Risk management practices are approved by management but may not be established as organizational-wide policy. . . .	There is an awareness of cybersecurity risk at the organizational level but an organization-wide approach to managing cybersecurity risk has not been established. Risk-informed, management-approved processes and procedures are defined and implemented, and staff has adequate resources to perform their cybersecurity duties. Cybersecurity information is shared within the organization on an informal basis.	The organization knows its role in the larger ecosystem, but has not formalized its capabilities to interact and share information externally.
Tier 3: Risk-Informed and Repeatable	The organization's risk management practices are formally approved and expressed as policy. Organizational cybersecurity practices are regularly updated based on the application of risk management processes to . . . a changing threat and technology landscape.	There is an organization-wide approach to manage cybersecurity risk. Risk-informed policies, processes, and procedures are defined, implemented as intended, and reviewed. Consistent methods are in place to respond effectively to changes in risk. Personnel possess the knowledge and skills to perform their appointed roles and responsibilities.	The organization understands its dependencies and partners and receives information from these partners that enables collaboration and risk-based management decisions within the organization in response to events.
Tier 4: Adaptive	The organization adapts its cybersecurity practices based on lessons learned and predictive indicators derived from previous . . . cybersecurity activities. Through a process of continuous improvement . . . the organization actively adapts to a changing cybersecurity landscape and responds to evolving and sophisticated threats in a timely manner.	There is an organization-wide approach to managing cybersecurity risk that uses risk-informed policies, processes, and procedures to address potential cybersecurity events. Cybersecurity risk management is part of the organizational culture and evolves from an awareness of previous activities, information shared by other sources, and continuous awareness of activities on their systems and networks.	The organization manages risk and actively shares information with partners to ensure that accurate, current information is being distributed and consumed to improve cybersecurity before a cybersecurity event occurs.

Fig. 2: NIST Framework Implementation Tiers Definitions[213]

213. *Id.* at 10–11.

C. Implementing the NIST Cybersecurity Framework

Articulating the basic components is only a portion of the Framework. Even more critical is how an organization implements the Framework. Understanding that organizations and industries vary significantly, and that cyber threats evolve rapidly, the Framework was developed in such a way as to allow implementation throughout myriad critical infrastructure settings.[214] First, the Framework was developed to be organizationally comprehensive, emphasizing coordination of the Framework throughout every level of an organization.[215] Second, the Framework was created to be flexible, allowing it to supplement an organization's already existing cybersecurity risk management program or to guide an organization in implementing such a risk management program for the first time.[216] Third, the Framework was organized to be adaptable to changing circumstances and environments so that future versions of the Framework could be created as the cybersecurity landscape evolves.[217]

The Framework stresses the coordination of risk management activities within every level of an organization.[218] Early on in the Framework's development, stakeholders emphasized the importance of the Framework's implementation into all levels of an organization—from senior leadership to employees, partners, and customers.[219] Thus, the Framework explains how the executive level, the business and process level, and the implementation and operations level of an organization can contribute to the implementation of the Framework.[220] Additionally, the Framework's flexibility is intended to allow its approach to address cybersecurity risks regardless of the organization, industry, or country.[221] As the Framework stresses, it is "not a one-size-fits-all approach to managing cybersecurity risk for critical infrastructure."[222] Instead, it assembles effective national and international cybersecurity practices, giving organizations the autonomy to adopt the Framework in a manner that fits the organization's business requirements and current risk management practices.

Further, because the NIST Framework "references globally recognized standards for cybersecurity, the Framework can also be used by organizations located outside the United States and can serve as a model for international

---

214. *See id.* at 4 (discussing the various considerations that went into the Framework, including making it adaptable for numerous different industries and businesses in various countries).

215. *Id.*

216. *Id.* at 6.

217. *See supra* text accompanying note 182.

218. *See* NIST CYBERSECURITY FRAMEWORK, *supra* note 2, at 12 & fig.2 (diagramming and discussing how executives, business/process level, and implementation/operations level personnel can simultaneously work toward improving cybersecurity).

219. *See* NAT'L INST. FOR STANDARDS & TECH., UPDATE ON THE DEVELOPMENT OF THE CYBERSECURITY FRAMEWORK (2013) (finding that the Cybersecurity Framework's Request for Information period stressed "the importance of senior leadership's engagement in the cybersecurity risk management process," and "[a]s a foundation, all users, including employees, partners, and customers, have a need for general cybersecurity awareness").

220. *See* NIST CYBERSECURITY FRAMEWORK, *supra* note 2, at 12 (describing a "common flow of information" and decision-making within an organization that includes all levels of an organization).

221. The Framework was importantly not intended to be United States-specific, and the Framework stresses that "the Framework can contribute to developing a common language for international cooperation on critical infrastructure cybersecurity." *Id.* at 4.

222. *Id.* at 2.

cooperation on strengthening critical infrastructure cybersecurity."[223] One region of significance is Europe. In 2013, a EU cybersecurity directive was proposed; it would require that companies harden their security policies to meet EU-developed standards—a development that could cause any firm providing online services in Europe to "fundamentally have to change the way its business operates."[224] Moreover, U.S.-EU policymakers are in regular discussions, meaning that the NIST Framework could be influential in shaping EU efforts in this space[225] and could even help shape a global duty of cybersecurity care—as is explored further in Part III.

The Framework provides a seven-step implementation process and may be used either as a reference guide to create a new risk management program or to supplement an already existing program.[226] For instance, AT&T has stated that it will begin assessing how the Framework "best complements [its] existing cyber-risk management program."[227] At the same time, IBM announced the creation of the IBM Industrial Controls Cybersecurity Consulting service that will assist companies in utilizing the Framework by "educat[ing] clients on details and mechanics of the NIST Cybersecurity Framework and perform[ing] a comprehensive assessment of a client's security maturity relative to the guidelines, best practices and international standards referenced in the Framework."[228]

Finally, the Framework's adaptability to changing circumstances allows it to evolve as the cybersecurity landscape continues to mature. The Framework is a "living document" that will be amended, updated, and improved as companies begin implementing the Framework and feedback begins to surface.[229] On the day the Framework was released, a "roadmap" was issued that discussed the Framework's "next steps" and identified "key areas of development, alignment, and collaboration."[230] NIST plans to relinquish its role as "convener and coordinator" to private industry, but it plans to continue its current leadership into at least version 2.0.[231]

---

223. *Id.* at 1–2.

224. *See* Warwick Ashford, *How Will EU Cyber Security Directive Affect Business?*, COMPUTERWEEKLY (Feb. 19, 2013), http://www.computerweekly.com/news/2240178256/How-will-EU-cybersecurity-directive-affect-business (citing Stewart Room, a partner at Field Fisher Waterhouse, who argues that this directive will mean that other firms beyond telecom companies will face regulatory burdens related to cybersecurity, including "e-commerce platforms; [I]nternet payment gateways; social networks; search engines; cloud computing services; and app stores").

225. *See generally EU Eying NIST Framework With 'Great Interest'*, *supra* note 30.

226. NIST CYBERSECURITY FRAMEWORK, *supra* note 2, at 13–15.

227. Ed Amoroso, *Protecting Our Nation's Critical Infrastructure*, AT&T PUB. POL'Y BLOG (Feb. 12, 2014), http://www.attpublicpolicy.com/cybersecurity/protecting-our-nations-critical-infrastructure/.

228. Press Release, IBM, IBM to Help Companies Utilize New Cybersecurity Framework Aimed at Protecting Nation's Critical Infrastructure (Feb. 13, 2014), http://www-03.ibm.com/press/us/en/pressrelease/43207.wss.

229. NIST CYBERSECURITY FRAMEWORK, *supra* note 2, at 2.

230. NAT'L INST. OF STANDARDS & TECH., NIST ROADMAP FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY 1 (2014), http://www.nist.gov/cyberframework/upload/roadmap-021214.pdf.

231. *Id.* at 1–2.

D. Framework Incentives and C-Cubed Voluntary Program

A difficulty with any voluntary program is encouraging participation. While advocated as a "cost-effective" approach,[232] implementing the Framework's practices will inevitably require time, money, and resources on the part of critical infrastructure organizations, especially those organizations that are currently without a cybersecurity risk management program. At the outset, increasing organizational participation in the Framework was approached in two ways: (1) reviewing current regulatory authorities to determine if establishing requirements based upon the Cybersecurity Framework would be permissible under current authority; and (2) researching a set of implementation incentives and developing a voluntary program to support the adoption of the Framework.[233]

First, Executive Order 13636 called on agencies with "responsibility for regulating the security of critical infrastructure [to] engage in a consultative process with [the] DHS, [the Office of Management and Budget], and the National Security Staff to review the . . . Framework and determine if current cybersecurity regulatory requirements are sufficient given current and projected risks."[234] These agencies are instructed to report to the President "whether or not the agency has clear authority to establish requirements based upon the Cybersecurity Framework to sufficiently address current and projected cyber risks to critical infrastructure, the existing authorities identified, and any additional authority required."[235]

However, not every organization that may fall within the ambit of "critical infrastructure" has clear regulatory requirements related to cybersecurity. To maintain the voluntary nature of the Framework, Executive Order 13636 tasked the Secretary of Homeland Security, "in coordination with Sector-Specific Agencies," to develop a "voluntary program" to support adoption of the Framework by critical infrastructure organizations and other interested entities.[236] Coinciding with the release of the Cybersecurity Framework, the DHS announced the Critical Infrastructure Cyber Community C³ Voluntary Program (C-Cubed Program).[237] The C-Cubed Program aims to "assist stakeholders with understanding use of the

232. NIST CYBERSECURITY FRAMEWORK, *supra* note 2, at 1.

233. Exec. Order No. 13636, 78 Fed. Reg. 11739, 11742–43 (Feb. 19, 2013).

234. *Id.* at 11742.

235. *Id.* at 11743. If current regulatory requirements were deemed "insufficient," agencies with responsibility for regulating the security of critical infrastructure are required to "propose prioritized, risk-based, efficient, and coordinated actions . . . to mitigate cyber risk." *Id.*

236. *Id.* at 11742–43. The Presidential Policy Directive 21 outlined the sixteen sectors of "critical infrastructure," as well as the "[s]ector-[s]pecific agency" that has "institutional knowledge and specialized expertise about the sector." Press Release, White House, Presidential Policy Directive—Critical Infrastructure Security and Resilience (Feb. 12, 2013), http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil. The critical infrastructure sectors established by the Directive, and their respective sector specific agencies, include: Chemical (DHS); Commercial Facilities (DHS); Communications (DHS); Critical Manufacturing (DHS); Dams (DHS); Defense Industrial Base (DoD); Emergency Services (DHS); Energy (Department of Energy); Financial Services (Department of Treasury); Food and Agriculture (Department of Agriculture and Department of Health and Human Services (DHHS)); Government Facilities (DHS and General Services Administration); Healthcare and Public Health (DHHS); Information Technology (DHS); Nuclear Reactors, Materials, and Waste (DHS); Transportation Systems (DHS and Department of Transportation); and Water and Wastewater Systems (Environmental Protection Agency). *Id.*

237. *Critical Infrastructure Cyber Community Voluntary Program*, US–CERT, http://www.us-cert.gov/ccubedvp (last visited Apr. 1, 2015).

Framework and other cyber risk management efforts, and support development of general and sector-specific guidance for Framework implementation."[238]

In addition to creating a voluntary program, Executive Order 13636 tasked the Secretary of Homeland Security, the Secretary of the Treasury, and the Secretary of Commerce with establishing "a set of incentives designed to promote participation in the Program."[239] The Departments' recommendations provided overlapping suggestions on how best to encourage the Framework's adoption[240] as well as consensus on eight recommendations: cybersecurity insurance, grant funds, government service process preferences, liability limitations, streamlining and unifying regulations, public recognition of voluntary participation, rate recovery for price regulated industries, and increased cybersecurity research.[241] Comments from the Obama Administration suggest it believes that market-based incentives and encouragement through the C-Cubed Voluntary Program will be the most successful drivers for organizations to adopt the Cybersecurity Framework. One senior Administration official stated:

> [W]e believe that the best drivers for adoption or use of the framework will ultimately be market based. Don't get me wrong, I think the government-based incentives are really important for us to pursue. But at the end of the day, it's the market that's got to drive the business case for the Cybersecurity Framework. The federal government is going to do its best to make the costs of using the framework lower, and the benefits of the framework higher, but it's the market that's going to ultimately make this work.[242]

As we will explore in Part III, however, market-driven incentives may be eclipsed not only by up-front costs but also by uncertainty—for instance, by creating incentives to avoid potential liability that may arise from failing to implement the Framework.

---

238. *Id.*

239. Exec. Order No. 13636, 78 Fed. Reg. at 11742.

240. *See* DEP'T OF COMMERCE, DISCUSSION ON RECOMMENDATIONS TO THE PRESIDENT ON INCENTIVES FOR CRITICAL INFRASTRUCTURE OWNERS AND OPERATORS TO JOIN A VOLUNTARY CYBERSECURITY PROGRAM 1–3 (2013) [hereinafter DEP'T OF COMMERCE RECOMMENDATIONS], *available at* http://www.ntia.doc.gov/files/ntia/ Commerce_Incentives_Discussion_Final.pdf (listing proposed government incentives to encourage adoption of the cybersecurity framework); DEP'T OF HOMELAND SEC., EXECUTIVE ORDER 13636: IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY 3 (2013) [hereinafter DHS STUDY], *available at* https://www.dhs.gov/ sites/default/files/publications/dhs-eo13636-analytic-report-cybersecurity-incentives-study.pdf ("Securing critical infrastructure against growing and evolving cyber threats requires a layered approach."); TREASURY DEP'T, SUMMARY REPORT TO THE PRESIDENT ON CYBERSECURITY INCENTIVES PURSUANT TO EXECUTIVE ORDER 13636, at 3–6 (2013) [hereinafter TREASURY DEP'T REPORT], *available at* http://www.treasury.gov/press-center/Documents/Treasury%20Report%20%28Summary%29%20to%20the%20President%20on%20Cybersecurity%20Incentives_FINAL.pdf (detailing numerous government incentives that could encourage the adoption of the cybersecurity framework).

241. Daniel, *Incentives*, *supra* note 19.

242. Press Release, White House, Background Briefing on the Launch of the Cybersecurity Framework (Feb. 12, 2014), http://www.whitehouse.gov/the-press-office/2014/02/12/background-briefing-launch-cybersecurity-framework.

E. Summary

This Part has explored the evolution and scope of the NIST Framework, investigating the reasons for its creation (namely Congressional inaction coupled with mounting cyber insecurity) and exploring its initial reception and uptake by critical infrastructure providers. The next task is linking this investigation to the legal analysis of Part I to begin exploring what impact the NIST Framework might have on delineating a global cybersecurity standard of care, which we conclude with next.

III. POTENTIAL FOR NIST CYBERSECURITY FRAMEWORK TO DEFINE NATIONAL AND INTERNATIONAL STANDARDS OF CYBERSECURITY CARE

As Part I demonstrated, legal compliance with current U.S. cybersecurity law relies heavily on interpreting and implementing "reasonable" and "appropriate" cybersecurity measures. Negligence law relies on oftentimes amorphous reasonable standards of care, while statutes like the GLBA require covered financial institutions to provide reasonable security safeguards. High-risk chemical facilities under the CFATS need to implement appropriate risk-based measures to mitigate cyber attacks in order to be compliant, while state breach notification statutes such as that of Massachusetts include clauses requiring governmental and private entities to implement reasonable data security measures. Given that what constitutes "reasonable" cybersecurity practices is not yet well defined, the NIST Cybersecurity Framework has the potential to be influential in shaping reasonable cybersecurity standards in the United States and further afield.

Like the United States, other nations and regions, including the United Kingdom, EU, and India, are in the midst of reshaping their own cybersecurity policies.[243] All of these jurisdictions have to date favored, to a greater or lesser degree, a more voluntary approach to enhancing cybersecurity, including for critical infrastructure companies, which could enhance the impact of the NIST Framework.[244] Indeed, because the NIST Framework "references globally recognized standards for cybersecurity," the drafters of the Framework created the instrument such that it may "also be used by organizations located outside the United States and can serve

243. *See, e.g.*, *EU Eying NIST Framework With 'Great Interest'*, *supra* note 30 (stating that the EU is trying to set up a cybersecurity framework and is considering the U.S. framework with great interest); Press Release, Cabinet Office & Francis Maude, Member of Parliament, Government Mandates New Cyber Security Standard for Suppliers (Sept. 26, 2014), http://www.gov.uk/government/news/ government-mandates-new-cyber-security-standard-for-suppliers (announcing that contractors bidding for some U.K. government contracts must comply with new "Cyber Essentials" controls); *NIST to Discuss Cybersecurity Framework with Officials from India*, INSIDE CYBERSECURITY (Sept. 16, 2014), http://insidecybersecurity.com/index.php?option=com_user&view=login&return=aHR0cDovL2luc21kZWN5YmVyc2VjdXJpdHkuY29tL0N5YmVyLURhaWx5LU5ld3MvRGFpbHktQnJpZWZzL25pc3QtdG8tZGlzY3Vzcy1jeWJlcnNlY3VyaXR5LWZyYW1ld29yay13aXRoLW9mZmljaWFscy1mcm9tLWluZGlhL21lbnUtaWQtMTA3NS5odG1s (reporting that the NIST is hosting Indian officials at a cybersecurity workshop to foster information exchanges about cybersecurity policies between the United States and India).

244. For more information on comparative critical infrastructure regulation, see generally Scott J. Shackelford & Amanda N. Craig, *Beyond the New "Digital Divide": Analyzing the Evolving Role of National Governments in Internet Governance and Enhancing Cybersecurity*, 50 STAN. J. INT'L L. 119 (2014).

as a model for international cooperation on strengthening critical infrastructure cybersecurity."[245]

Although the time is not yet ripe to tell a definitive story of the national, to say nothing of the global, impact of the NIST Framework given how recently the Framework was announced prior to this writing, it is important to begin a conversation—especially given the centrality of due diligence standards in building out norms that would contribute to a law of cyber peace applicable below the armed attack threshold.[246] Although norms may not bind states in the same manner as formalized treaties, as Jim Lewis of the Center for Strategic and International Studies has noted, "[N]on-binding norms [can] exercise a powerful influence on state behaviour."[247] Indeed, the importance of norms to enhancing cybersecurity has been referenced in numerous international conferences[248] and in academia.[249] In particular, due diligence standards, which may be considered to be a core area of cybersecurity that the NIST Framework is designed to strengthen, have been touted as a vital cyber norm to better define.[250] To that end, this Part examines three case studies—the United Kingdom, the EU, and India—to begin the analysis of how the NIST Framework may help shape a regional, if not global, cybersecurity standard of care for critical infrastructure firms. Finally, it assesses the role that the private sector might play in promoting the Framework globally.

A. The NIST Cybersecurity Framework and Shaping a Reasonable Standard of Care

The NIST Framework could have a particularly significant impact on shaping a reasonable standard of cybersecurity care in common law negligence claims. What exactly is "reasonable" is itself open to interpretation. Courts, however, have found that it does not necessarily infer "state of the art" facilities, technologies, or business

245. NIST CYBERSECURITY FRAMEWORK, *supra* note 2, at 1–2.

246. *See* Scott J. Shackelford, *From Nuclear War to Net War: Analogizing Cyber Attacks in International Law*, 27 BERKELEY J. INT'L L. 192, 229–32 (2009) (introducing the international law applicable above and below the armed attack threshold, which is the point above which the law of war is activated).

247. James Andrew Lewis, *Confidence-Building and International Agreement in Cybersecurity*, *in* DISARMAMENT FORUM: CONFRONTING CYBERCONFLICT 51, 53 (2011).

248. *E.g.*, Rep. of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 65th Sess., Sept. 14, 2010–Sept. 12, 2011, para. 18, U.N. Doc. A/65/201 (July 30, 2010). For example, in 2007, the International Telecommunications Union (ITC) held a cybersecurity workshop to bring together West African stakeholders "to discuss, share information, and collaborate on the elaboration and implementation of national policy, regulatory and enforcement frameworks for cybersecurity and CIIP," also known as critical information infrastructure protection. *ITU West Africa Workshop on Policy and Regulatory Frameworks for Cybersecurity and Critical Information Infrastructure Protection (CIIP)*, INT'L TELECOMM. UNION, http://www.itu.int/ITU-D/cyb/events/2007/praia/ (last visited Apr. 2, 2015).

249. *See, e.g.*, ROGER HURWITZ, AN AUGMENTED SUMMARY OF THE HARVARD, MIT AND U. OF TORONTO CYBER NORMS WORKSHOP 8–10 (2012) (outlining the difficulty of building consensus around international cybersecurity norms at a large academic workshop).

250. *See, e.g.*, Andreas Zimmermann, *International Law and 'Cyber Space'*, ESIL REFLECTIONS, Jan. 2014, at 1, 4, *available at* http://www.esil-sedi.eu/sites/default/files/ESIL%20Reflections%20-%20Andreas%20Zimmermann_0.pdf (noting that there are many unanswered legal questions related to the specific content of due diligence obligations in cyber space).

practices.[251] Because of the ambiguity that can surround reasonableness, reliance on industry standards has been used "as a guidepost for assessing reasonable conduct."[252] As has been stated, "Company practices and procedures should be rooted in concepts of reasonableness. Adherence to industry practice, in turn, may be viewed as reasonable and provide a defense in some cases in the event of litigation."[253]

When viewed through the lens of Judge Hand's risk/utility formula discussed in Part I,[254] the Cybersecurity Framework could provide a new basis on which courts utilize the formula, particularly in determining how "adequate" the Framework might have been to prevent alleged harm and the "burden" on an organization to implement the Framework. The Framework, again, is not a new set of standards or best practices for critical infrastructure organizations but instead provides a way for companies to determine which standards and practices are worth implementing and whether an organization is adequately doing so through its current risk management process. The Framework's approach to applying common cybersecurity practices could be an "adequate precaution" to mitigate cybersecurity threats that, if successful, could result in harm to the nation's security, the economy, or the public's safety. Courts could also look at what the "burden" on an organization might have been to use the Framework to determine which cybersecurity practices were best suited for their particular industry. Overall, a critical infrastructure organization could be found to have acted negligently if it is determined that (1) the critical infrastructure organization suffered a cyber attack that resulted in damage or injury; (2) the organization failed to utilize the Framework to address and manage its cybersecurity risks; (3) the Framework is deemed an adequate precaution that, if implemented, would have prevented the harm; and (4) the burden on an organization to utilize the Framework was less than the probability that the cybersecurity incident would occur multiplied by the significance of the incident.

Outside of a risk/utility analysis, reliance on industry standards to determine what constitutes reasonable cybersecurity practices leaves ample room for utilization of the NIST Framework. Similar to the FFIEC report in *Shames–Yeakel*,[255] the NIST Cybersecurity Framework could be utilized to argue the appropriate standard of care. Failing to comply with the NIST Framework, similar to Citizens Financial Bank's delayed compliance with the recommended multi-factor authentication in the FFIEC report or Sony's failure to employ industry encryption standards,[256] could be enough to establish a triable issue of fact as to whether reasonable standards of cybersecurity have been met by a company (meaning that courts would not be able to establish as a matter of law that a company adhered to a reasonable standard of care). Overall, cases like *Shames–Yeakel* and the many cases deriving from the 2011 Sony breach demonstrate just how fertile the ground is for defining a reasonable

251. *See, e.g.*, Ross v. RJM Acquisitions Funding LLC, 480 F.3d 493, 496–99 (7th Cir. 2007) (analyzing the term "reasonable" under the Fair Debt Collection Practices Act). *Ross* is not a security case and thus is limited in its authoritative value. However, the Fair Debt Collection Practice Act, which the court is interpreting, may be used as persuasive authority in the context of technological safeguards. ANDREW B. SERWIN, INFORMATION SECURITY AND PRIVACY: A GUIDE TO FEDERAL AND STATE LAW AND COMPLIANCE § 24:96 (2014).

252. IAN BALLON, E-COMMERCE AND INTERNET LAW: TREATISE WITH FORMS § 2.05 (2014).

253. *Id.*

254. *See supra* notes 58–65 and accompanying text.

255. *See supra* notes 84–87 and accompanying text.

256. *See supra* notes 71–76 and accompanying text.

standard of cybersecurity care—and just how cogently the Cybersecurity Framework could fulfill that role depending on industry uptake and ultimate judicial interpretation.

Attempts to utilize the Framework under a negligence theory would still need to overcome the other hurdles plaguing data security cases. Hurdles—such as establishing Article III standing and overcoming the economic loss doctrine—have often prevented in-depth judicial analysis of the standard of care issue in data security negligence cases.[257] That being said, if the consequences of lax security measures go beyond breach of sensitive data and produce kinetic effects impacting the health, safety, and welfare of individuals, then plaintiffs attempting to recover from mere data breaches will likely be able to overcome some of these hurdles.[258] As a result, courts would have the opportunity to grapple more directly with the standard of care issue.

In addition to its impact on common law, the Cybersecurity Framework could shape statutorily enumerated requirements on organizations to implement reasonable cybersecurity requirements. As Part I demonstrated, many statutory and regulatory requirements do not mandate specific practices, but instead provide space for an organization to assess its own cyber risks and implement reasonable safeguards.[259] Similar to negligence and fiduciary law, the NIST Framework's collection of industry practices to identify, protect, detect, respond, and recover from cybersecurity risks could thus set the standard for what constitutes reasonable cybersecurity practices within these statutory regimes.

To date, the Administration has continued to push for a voluntary approach to the Framework's adoption,[260] thus making it unlikely that regulators will use their enforcement authority against covered entities that fail to voluntarily utilize the NIST Framework. After assessing the sufficiency of existing regulatory authority to establish requirements based on the Cybersecurity Framework, as ordered by Executive Order 13636, the President's Cybersecurity Coordinator, Michael Daniel, announced that "existing regulatory requirements, when complemented with strong voluntary partnerships, are capable of mitigating cyber risks to our critical systems and information."[261] Reviews conducted by the Environmental Protection Agency,[262]

257. *See supra* notes 88–91 and accompanying text.

258. *See, e.g.*, Fahmida Y. Rashid, *Chinese Hackers Attacked FEC During Government Shutdown*, PC MAG. SECURITY WATCH (Dec. 17, 2013), http://securitywatch.pcmag.com/hacking/318975-chinese-hackers-attacked-fec-during-government-shutdown (reporting on a massive hack on the Federal Election Commission (FEC) that "crashed several FEC computer systems" while IT personnel were furloughed during the 2013 government shutdown); *see also* WATER SECTOR COORDINATING COUNCIL CYBER SEC. WORKING GRP., ROADMAP TO SECURE CONTROL SYSTEMS IN THE WATER SECTOR 16 (2008) (listing "real cyber events" that resulted in kinetic consequences involving water sector organizations).

259. *See supra* Part I.C.

260. *See supra* Part II.

261. Michael Daniel, *Assessing Cybersecurity Regulations*, WHITE HOUSE BLOG (May 22, 2014), http://www.whitehouse.gov/blog/2014/05/22/assessing-cybersecurity-regulations.

262. *See, e.g.*, Letter from Peter C. Grevatt, Dir., U.S. Envt'l Prot. Agency Office of Ground Water & Drinking Water, to Michael Daniel, http://water.epa.gov/infrastructure/watersecurity/upload/EO_13696_10-b-_EPA_response.pdf ("[T]he EPA believes that a voluntary partnership model is a proven approach that will be effective for managing cybersecurity risks . . . .").

the Department of Health and Human Services,[263] and the DHS[264] all generally supported the voluntary approach to addressing and mitigating cyber risks. However, the voluntary approach could very well shift to a more mandatory approach if the current implementation policies are found to be ineffective.[265] Some critical infrastructure organizations, recognizing the consistency between the Cybersecurity Framework and existing regulatory requirements like the GLBA, HIPAA, and CFATS, are proactively reviewing their cybersecurity risk management practices to reflect both the Framework and their existing regulatory requirements.[266] Although potentially beneficial, such an extra level of due diligence also increases the time and resources these organizations must take to ensure compliance, as is discussed further below.[267]

Beyond regulatory enforcement, however, federal requirements on organizations to implement cybersecurity requirements could be used to impose liability through the legal doctrine of negligence per se. Negligence per se is a "theory of negligence in which the fact that an entity's conduct has violated some applicable statute is *prima facie* evidence that the entity has acted negligently."[268] In other words, conduct that violates a statute satisfies the "duty" and "breach" elements of a plaintiff's negligence claim. "In the context of cyber threats to critical infrastructure," a Congressional Research Service report on critical infrastructure liability has stated, "a regulated entity that fails to adequately secure its information infrastructure as required under a federal regulatory scheme [may be] liable for a cyber incident that causes harm to customers or other third parties."[269] If the NIST Framework is utilized as a benchmark for the various sector-specific cybersecurity requirements, an organization may not only face penalties from a federal regulator but also may be open to negligence per se–based lawsuits. However, the utilization

263. *See, e.g.*, Press Release, Dep't of Health and Human Servs., HHS Activities to Enhance Cybersecurity: Executive Order 13636, Section 10(b)—HHS Assessment (May 12, 2014), http://www.phe.gov/Preparedness/planning/cip/Pages/eo13636.aspx ("Through these programs, HHS works in voluntarypartnership with public and private sector entities . . . to enhance their security and resilience with respect to all hazards, including cyber threats.").

264. *See, e.g.*, DEP'T OF HOMELAND SEC., EXECUTIVE ORDER 13636—IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY SECTION 10(B) REPORT ON THE DEPARTMENT OF HOMELAND SECURITY'S CHEMICAL FACILITY ANTI-TERRORISM STANDARDS (2014), *available at* http://www.dhs.gov/sites/default/files/publications/EO%2013636%20Section%2010%28b%29%20Report%20for%20CFATS%20%28May%202014%29%20Final_0.pdf (discussing various proposals that "have value as part of an overall approach to risk management," which led DHS to "encourag[e] high-risk chemical facilities to consider the voluntary adoption" of NIST Framework protocols).

265. *Cf. Cyber Regulatory Landscape Could Be More Nuanced than Acknowledged*, INSIDE CYBERSECURITY (May 19, 2014), http://insidecybersecurity.com/Cyber-General/Cyber-Public-Content/cyber-regulatory-landscape-could-be-more-nuanced-than-acknowledged/menu-id-1089.html ("[T]he White House is broadly asserting, without disclosing details, that federal regulators are confident their existing authority is adequate to implement the president's cybersecurity executive order.").

266. *See, e.g.*, Joe Adler, *Why Obama's "Voluntary" Cybersecurity Plan May Prove Mandatory*, AM. BANKER, Feb. 14, 2014, http://www.americanbanker.com/issues/179_32/why-obamas-voluntary-cybersecurity-plan-may-prove-mandatory-1065651-1.html (finding that the financial sector expects regulators to incorporate the cybersecurity framework in their requirements for financial institutions, likely by cross-referencing it to the privacy and security obligations under the GLBA).

267. *See infra* notes 316–325 and accompanying text.

268. LIU ET AL., *supra* note 20, at 6 (citing Makas v. Hillhaven, Inc., 589 F. Supp. 736, 741 (M.D.N.C. 1984)).

269. LIU ET AL., *supra* note 20, at 6.

of the negligence per se standard still falls prey to the other negligence hurdles the plaintiff must satisfy, including satisfying standing requirements, making it somewhat difficult to employ negligence per se in a cybersecurity context.[270]

Beyond federal regulatory requirements, state laws that call for "reasonable" security measures for certain types of personal information may also provide an opportunity for the Cybersecurity Framework to play a part in shaping what constitutes reasonable standards of cybersecurity care. Organizations operating within a particular state—especially those that use or store personal information as defined under state law—need to also be aware of the potential for liability that state statutes might create. This also reflects general security requirements that supplement state breach notification laws. Organizations that fail to utilize the Framework and suffer a breach that compromises a particular state's citizens' personal information may be open to regulatory action by the appropriate state authorities under an argument that the company has failed to implement "reasonable" security measures. In addition, some states are looking to explicitly require through legislation utilization of the Cybersecurity Framework now that the Framework has been released.[271]

Regardless of the Framework's eventual impact on a reasonable standard of cybersecurity care, the uncertainty of legal consequences may be enough to hinder private-sector voluntary participation in the Framework.[272] Legal compliance issues have typically dominated business approaches to cyber threats. A 2013 survey by AIG and Penn Schoen Berland, for instance, found that 75% of executives and brokers said that "legal compliance issues are making companies think more about cyber risks."[273]

This focus on legal compliance has prompted a push for congressional action that could limit the liability of organizations that implement the Framework. The incentive reports issued by the DHS, the Department of Commerce, and the Department of the Treasury all included discussion on some form of limited liability for companies who voluntarily adopt the Framework.[274] The Commerce Department, for instance, suggested that the Framework should:

> include a review of tort cases against critical infrastructure owners and operators and an assessment of mechanisms . . . that have the potential to

---

270. *See* Rustad & Koenig, *Extending Hand's Formula*, *supra* note 65, at 241 (stating that, at the time of the article's publication, "[n]o plaintiff has successfully employed a *negligence per se* argument in a computer security case").

271. *See, e.g.*, H.B. 804, 434th Gen. Assemb., Reg. Sess. (Md. 2014) (proposing to require Maryland to include a cybersecurity framework within its information technology master plan, and for that framework to consider materials developed by the NIST).

272. Lauren Larson, *NIST, DHS Push for More Engagement Around Cyber Framework*, FEDERAL NEWS RADIO (Mar. 27, 2014), http://www.federalnewsradio.com/473/3591100/NIST-DHS-push-for-more-engagement-around-cyber-framework- (reporting statements of Wisconsin Senator Ron Johnson that "fear of legal entanglements may be hindering participation" in the NIST framework).

273. Press Release, Am. Int'l Grp., Inc., AIG Survey Finds More Insurance Decision Makers Concerned about Cyber Threat than Other Major Risks (Feb. 6, 2013), http://phx.corporate-ir.net/phoenix.zhtml?c=76115&p=irol-newsArticle&ID=1782195&highlight=.

274. DEP'T OF COMMERCE RECOMMENDATIONS, *supra* note 240, at 14–15; DHS STUDY, *supra* note 240, at 62–63; TREASURY DEP'T REPORT, *supra* note 240, at 3.

> reduce or transfer their tort liability if a cyber incident causes damage despite the owner or operator's adoption and implementation of some or all of the standards, procedures, and other measures that comprise the Framework.[275]

Fear of liability is also a reason why many recent cybersecurity legislative proposals have included limits on legal liability for organizations that implemented the proposed framework.[276] Until these legal uncertainties are addressed, the Administration's aspirational goals of widespread utilization of the Framework may prove futile.

Of course, a different outcome is also conceivable. The legal uncertainty surrounding the Framework's impact on legal liability could be an incentive for organizations to begin implementing the Cybersecurity Framework. Given the ambiguity as to how exactly a reasonable standard of cybersecurity care may be taking form, implementation of the Framework could be viewed by companies as the most efficient way to mitigate risk to legal liability. So while some fear that the Framework may be used as a sword by plaintiffs,[277] companies may look to the Framework for its use as a liability shield, arguing that, despite the occurrence of cyber attacks resulting in harm, an organization's utilization of the Framework translated into reasonable security measures under the circumstances and could therefore mitigate liability. Companies though may still look to government to make this "safe harbor" concept explicit through congressional action given the absence of comprehensive U.S. cybersecurity legislation.

B. Voluntary Cybersecurity Frameworks in Global Context

The lack of clarity regarding what constitutes a standard of cybersecurity care in the United States is further muddled when comparing the situation in the U.S. with that of other jurisdictions. Still, analyzing national regulation in cyberspace is important for at least three reasons: (1) national control of cyberspace is increasing and is a critical aspect of its status as a "pseudo commons,"[278] (2) enclosure through

---

275. DEP'T OF COMMERCE RECOMMENDATIONS, *supra* note 240, at 2.

276. *E.g.*, Cybersecurity Act of 2012, S. 3414, 112th Cong. § 706 (2012).

277. *See, e.g.*, Chris Strohm, *US Unveils Cyber Security Guidelines for Industry*, HYDROCARBON PROCESSING (Feb. 14, 2014), http://www.hydrocarbonprocessing.com/Article/3309410/Latest-News/US-unveils-cyber-security-guidelines-for-industry.html (quoting a lawyer who sees the potential for a company's non-adoption of the framework leading to a "presumption of negligence" against the company).

278. The pseudo commons represents a compromise position between competing models of cyber regulation, namely those espousing Internet sovereignty and Internet freedom, i.e., considering cyberspace as an extension of national territory or a global networked commons. *See, e.g.*, David R. Johnson & David G. Post, *Law and Borders–The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367, 1375 (1996) ("The rise of an electronic medium that disregards geographical boundaries throws the law into disarray by creating entirely new phenomena that need to become the subject of clear legal rules but that cannot be governed, satisfactorily, by any current territorially based sovereign."); Lawrence Lessig, *The Law of the Horse: What Cyberlaw Might Teach*, 113 HARV. L. REV. 501, 519 (1999) ("The limitations on the scope of intellectual property law serve to fuel the intellectual commons—to generate a resource upon which others can draw."); *see also* JOSEPH S. NYE, JR., THE FUTURE OF POWER 143 (2011) (referring to cyberspace as an "imperfect commons"); Press Release, Ind. U., London Conference Reveals 'Fault Lines' in Global Cyberspace and Cybersecurity Governance (Nov. 7, 2011), *available at* http://newsinfo.iu.edu/news/page/normal/20236.html (highlighting the tension between civil liberties and regulations online).

nationalization is one of the classic solutions to the tragedy of the commons,[279] and (3) national regulations form an important component of polycentric governance—a useful vehicle for conceptualizing cybersecurity law and policy—even though states do not enjoy a "general regulatory monopoly" in cyberspace.[280] The importance of investigating national regulation comes into sharp relief in the context of the NIST Framework, especially given the extent to which it could catalyze positive network effects, enhancing cybersecurity across sectors and borders.[281]

1. U.K. Cybersecurity Frameworks

In the United Kingdom, as in the United States, the emphasis to date has been on voluntary standards to enhance Critical National Infrastructure protection. For example, the 2011 U.K. Cyber Security Strategy, which focuses on government contractors, states that the British government "will work with industry to develop rigorous cyber security . . . standards."[282] In addition, the United Kingdom's Centre for the Protection of National Infrastructure (CPNI) published "a baseline of high-priority information security measures and controls that can be applied across an organisation in order to improve its cyber defence."[283] However, the Strategy neglects to explain how the largely voluntary approach represents a significant change to the status quo sufficient to effectively meet this threat to British national security,[284] and the information security controls are labeled specifically as "guidance."[285] The Strategy also does not offer specifics about how the British government will help enhance cybersecurity for the "wider group of companies not currently deemed part of the critical infrastructure" but which are nevertheless essential to Britain's long-term economic competitiveness.[286] However, the United Kingdom has announced plans for a new strike force capable of protecting public and private sector assets against cyber attacks.[287]

---

279. *See, e.g.*, Antonio Lambino, *Impending Tragedy of the Digital Commons?*, WORLD BANK (Oct. 25, 2010), http://blogs.worldbank.org/publicsphere/node/5562 (discussing the tendency of governments to intervene in computer networks in the interest of national security).

280. ANDREW D. MURRAY, THE REGULATION OF CYBERSPACE: CONTROL IN THE ONLINE ENVIRONMENT 47 (2007). For more on the role that polycentric governance can play in enhancing cybersecurity, see Scott J. Shackelford, *Toward Cyberpeace: Managing Cyberattacks through Polycentric Governance*, 62 AM. U. L. REV. 1273 (2013).

281. *Cf.* Neal K. Katyal, *The Dark Side of Private Ordering: The Network/Community Harm of Crime*, *in* THE LAW AND ECONOMICS OF CYBERSECURITY 193, 193–94 (Mark F. Grady & Francesco Parisi eds., 2006) ("The Internet is the paradigmatic sphere in which the positive advantage of 'network effects' is central—that the greater the size of the network, the greater the benefits.").

282. U.K. CABINET OFFICE, THE UK CYBER SECURITY STRATEGY: PROTECTING AND PROMOTING THE UK IN A DIGITAL WORLD 27 (2011), *available at* https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf (emphasis omitted).

283. *Critical Security Controls Guidance*, CTR. FOR PROTECTION OF NAT'L INFRASTRUCTURE, http://www. cpni.gov.uk/advice/cyber/Critical-controls/ (last visited Apr. 2, 2015).

284. *See generally* U.K. CABINET OFFICE, *supra* note 282.

285. *Critical Security Controls Guidance*, *supra* note 283.

286. U.K. CABINET OFFICE, *supra* note 282, at 28.

287. Rob Waugh, *New British Cyber Defense Force Will Protect Industry—And "If Needed, Strike in Cyberspace"*, WELIVESECURITY (Sept. 29, 2013), http://www.welivesecurity.com/2013/09/29/new-british-cyber-defense-force-will-protect-industry-and-if-needed-strike-in-cyberspace/.

How might the NIST Framework impact the current state of the United Kingdom's cybersecurity policymaking? Given the common legal origins of U.S. and U.K. law, the analysis of negligence jurisprudence in the United States should be informative, if not dispositive, to British firms in weighing whether to invest in considering their compliance with measures or controls advanced by the CPNI or resulting from the Cyber Security Strategy. If such controls are recognized as establishing some grounds for a negligence case, CPNI or another government agency might also be encouraged to develop more detailed cybersecurity standards like those included in the NIST Framework, in which case the Framework may be considered a useful starting point. This outcome may even be more likely in the United Kingdom than in the United States given the lower barriers to standing prevalent in British common law.[288] This might potentially open up the courts to negligence lawsuits, for example, to a greater degree than what has been witnessed to date in the United States. Likewise, the role that U.S. executive agencies are playing in potentially expanding the scope of industries affected by the Framework's standards might demonstrate how the British government could move beyond developing standards relevant only to critical infrastructure. But the biggest looming change for British cybersecurtity policymaking might not be coming from across the Atlantic but from across the English Channel.

2. EU Cybersecurity and NIST

In 2013 an EU cybersecurity directive was proposed requiring companies to harden their cybersecurity to meet EU-developed standards—a development that could cause any firm providing online services in Europe to "fundamentally have to change the way its business operates."[289] Among much else, this regime would require many firms with some nexus to e-commerce to invest in cybersecurity technologies, develop procedures to prove compliance to national and EU regulators, and undertake enhanced cyber risk mitigation measures to better manage attacks.[290] It could also help define a Europe-wide cybersecurity duty of care for covered industry. Given that the size of the EU's economy is comparable, if not larger, than that of the United States,[291] this new EU regime could have substantive

288. *See, e.g.*, Jon Owens, *Comparative Law and Standing to Sue: A Petition for Redress for the Environment*, 7 ENVNTL. L. 321, 325–26 (2001) (comparing the "overseas trend in favor of broader standing" with the United State's more restrictive standing doctrine).

289. Ashford, *supra* note 224.

290. *Id.*; *see also Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, at 2–6, JOIN (2013) 1 final (Feb. 7, 2013) (espousing an Internet freedom agenda including universal access, democratic and "efficient multi-stakeholder governance," and setting out goals to achieve "cyber resilience"; to achieve this, the Communication sets out a number of goals, including setting national-level cybersecurity standards, setting up national and regional CERTs, sharing private-sector best practices, and regularly assessing cyber risk—especially for firms operating critical infrastructure—so as to build a "cybersecurity culture"). *But see* Stephen Gardner, *Member States Reportedly Unconvinced on Need for EU Cybersecurity Directive*, BLOOMBERG BNA (June 3, 2013), http://www.bna.com/member-states-reportedly-n17179874317/ (reporting on questions from ministers arising from a mandate approach and noting that "other parts of the world, such as the USA, appear to opt for a more voluntary and flexible approach with regard to cybersecurity standards" and worrying about creating "inconsistencies for companies whose operations span several jurisdictions" (internal quotations omitted)).

291. *See The Economy*, EUR. UNION, http://europa.eu/about-eu/facts-figures/economy/index_en.htm

network effects extending to the many global businesses that operate in EU nations.[292]

What has been less appreciated to date is the impact that the NIST Framework could have on this burgeoning EU cybersecurity policy. According to Francois Rivasseau, the Deputy Head of the EU delegation to the United States, "European officials are considering the [NIST] framework . . . with 'great interest.'"[293] Indeed, Rivasseau went on to note: "The EU is is [sic] trying to set up a European system that 'would basically provide us with the same capabilities or possibilities,'" further mentioning that the NIST Framework should be a "catalyst[]" that "lead[s] to the creation of [cybersecurity] norms."[294] Though formal European endorsement of the NIST Framework has not yet occurred as of writing, there are ongoing discussions about how best to translate the NIST Framework for use by global audiences.[295] Most importantly, many of the Framework's guidelines can be mapped to International Organization for Standardization (ISO) standards (like ISO/IEC 27001:2013 at 32)[296] or Control Objectives for Information and Related Technology 5 (COBIT 5) standards, which were developed by a global industry association.[297] Such standards represent global best practices,[298] meaning that EU adoption can be framed as compliance with international standards that protect global business. As such, these European efforts could be deemed to reinforce the NIST Framework and help to bolster its global impact.

(last visited Apr. 2, 2015) (noting that the EU's economy is larger than the United States's economy in terms of the goods and services that it produces).

292. *See, e.g.*, Agustino Fontevecchia, *The Largest U.S. Companies with Big European Exposure*, FORBES (Nov. 9, 2011), http://www.forbes.com/sites/afontevecchia/2011/11/09/defensive-stocks-like-coke-and-ge-far-from-immune-to-europe/ (noting that the EU's slowing economy "will affect U.S. companies with substantial sales exposure to the Old Continent").

293. *EU Eying NIST Framework With 'Great Interest'*, *supra* note 30.

294. *Id.*

295. *See id.* (acknowledging that the EU was considering the NIST Framework, although expressing uncertainty as to whether formal adoption of the Framework would be forthcoming); *see also* Dan Verton, *Global Security Association Helps Translate NIST Framework*, FEDSCOOP (Sept. 15, 2014, 4:41 PM), http://fedscoop.com/global-security-association-helps-explain-nist-framework/ (noting that the Information Security Forum, a U.K. based association, has released a mapping document to help companies understand where their level of compliance with the NIST network falls).

296. The ISO has also developed guidance "to help various industry sectors use the organization's recently updated standards for information technology security." *International Group Drafts Guidance to Encourage Cross-Sector Use of New Security Standards*, INSIDE CYBERSECURITY (Feb. 3, 2014), http://insidecybersecurity.com/Cyber-Daily-News/Daily-News/international-group-drafts-guidance-to-encourage-cross-sector-use-of-new-security-standards/menu-id-1075.html.

297. *See* Press Release, ISACA, New US Cybersecurity Framework Developed by NIST Features COBIT 5 in the Core (Feb. 14, 2014), http://www.isaca.org/About-ISACA/Press-room/News-Releases/2014/Pages/New-US-Cybersecurity-Framework-Developed-by-NIST-Features-COBIT-5-in-the-Core.aspx (noting that the ISACA helped in the development of the NIST Framework, which can be mapped back to "COBIT due to its global relevance and proven industry use").

298. *See, e.g.*, Gary Hardy, *Guidance on Aligning CobiT, ITIL, and ISO 17799*, 1 INFO. SYSTEMS CONTROL J. 1, 1–2 (2006), http://www.isaca.org/Journal/archives/2006/Volume-1/Documents/jpdf0601-Guidance-on-Aligning.pdf (stating that ISO and COBIT apply generally to all IT best practices).

3. Voluntary Cybersecurity Frameworks in India

Similar to the EU, and also in 2013, India published its first policy explicitly devoted to protecting critical information infrastructure: the National Cyber Security Policy 2013 (NCSP).[299] The 2013 policy calls for the creation of a National Critical Information Infrastructure Protection Centre (NCIIPC) to protect critical infrastructure,[300] while section IV.A in particular "encourage[s]" all organizations to designate a chief information security officer and "to develop information security policies duly integrated with their business plans and implement such policies as per international best practices."[301] Section IV.B further promotes the adoption of global best practices "in information security and compliance" and "in formal risk assessment and risk management processes."[302] While the 2013 NCSP is mostly devoted to explaining the role that the Indian government should play in protecting critical information infrastructure, the NCIIPC in June 2013 also published Guidelines for the Protection of National Critical Information Infrastructure, which are more targeted to India's private sector but similarly reference the importance of adhering to global standards.[303] However, the NCIIPC lacks a "public face," and its "exact functions" are in doubt,[304] rendering dubious its potential to encourage private sector adoption of its Guidelines.

The NCSP and Guidelines for the Protection of National Critical Information Infrastructure, then, are reminiscent of U.S. and U.K. efforts at establishing voluntary cybersecurity best practices—rather than the more heavy-handed EU approach. But both documents' explicit and numerous references to global standards and best practices create an opportunity for government officials and businesses promoting the NIST Framework to refer to its ISO and COBIT 5 standards references. Moreover, if Europe develops an approach that strengthens the Framework abroad, and given India's common law roots with U.K. jurisprudence, then Indian firms may be more strongly encouraged to implement the NIST Framework or the global standards that it references. In addition, the United States may be encouraging adoption of the Framework or such standards more directly; in December 2013, India's Ministry of Home Affairs conducted its first "homeland security dialogue" with the U.S. government, during which the countries discussed the need to build secure cyber infrastructure and "synchronize" domestic laws with

299. MINISTRY OF COMMC'N & INFO. TECH., NOTIFICATION ON NATIONAL CYBER SECURITY POLICY—2013, FILE NO. 2(35)/2011-CERT-IN (2013) (India) [hereinafter 2013 NCSP]; *Government Releases National Cyber Security Policy 2013*, TIMES OF INDIA, July 2, 2013, http://articles.timesofindia.indiatimes.com/2013-07-02/security/40328016_1_national-cyber-security-policy-power-infrastructure-air-defence-system; *National Cyber Security Policy: An Analysis*, CALIBRE (July 3, 2013), http://thecalibre.in/in-depth-current-affairs/national-cyber-security-policy-an-analysis/072013/?p=3853 [hereinafter Calibre Analysis].

300. Calibre Analysis, *supra* note 299.

301. 2013 NCSP, *supra* note 299, § IV.A(3).

302. *Id.* § IV.B(1), (3).

303. *See* Muktesh Chander, *Protection of National Critical Information Infrastructure*, DEF. & SECURITY ALERT, Oct. 2013, at 54, 55–56, *available at* http://www.dsalert.org/images/web/intro/October_2013_Issue_Intro.pdf (providing general information about CII, detailing international efforts and NCIIPC's efforts to protect CII).

304. *NTRO Would Protect the Critical ICT Infrastructures of India*, CTR. OF EXCELLENCE FOR CYBER SECURITY RESEARCH & DEV. INDIA (Jan. 13, 2014) (on file with author).

global standards.[305] However, it is not only national policymakers who are paying attention to the roll out of the NIST Framework. Perhaps even more involved to date have been companies,[306] both in the drafting and now the global push to establish a global cybersecurity duty of care and contribute to the process of cyber norm creation. It is to that story that we turn to next.

C. How (and Why) the Private Sector is Pushing the NIST Framework Globally

Since its publication in February 2014, the NIST Framework has been heralded by both U.S. industry and government officials as an example of leveraging public-private partnerships to achieve effective cybersecurity policy.[307] Indeed, while drafting the Framework, NIST requested and incorporated feedback from more than 3000 security professionals.[308] Because some U.S. technology companies and industry associations have "invested considerable time and energy toward developing the [F]ramework"—and already believe themselves to be in compliance with the Framework—they are motivated not only to demonstrate their "commitment to using the [F]ramework" but also to promote the Framework.[309] Broader adoption of the Framework may not only lead to greater resilience, enabling continued wide use of companies' information security products, but also enable them to demonstrate a competitive advantage.

Industry association ISACA, which represents 110,000 cybersecurity, governance, and assurance professionals, assisted NIST in the development of the Framework and gave NIST a platform to present at ISACA's North American Computer Audit, Control and Security Conference in April.[310] Likewise, numerous

---

305. Press Release, Press Info. Bureau, Gov't of India, Ministry of Home Affairs, India-US Homeland Security Dialogue Two Day Conference of Police Chiefs Concludes (Dec. 5, 2013), http://pib.nic.in/newsite/PrintRelease.aspx?relid=101040. Notably, though, what government agency might best develop and implement critical infrastructure best practices remains unclear. In India, the Department of Electronics and Information Technology, Department of Telecom, Ministry of Defense, Ministry of Home Affairs, and National Security Advisor (Prime Minister's Office) are all important stakeholders.

306. *E.g.*, Press Release, IBM, *supra* note 228 (introducing and discussing NIST's new Cybersecurity Framework, in relation to IBM's cybersecurity consulting service).

307. *E.g.*, INFO. TECH. INDUS. COUNCIL, ITI RECOMMENDATIONS TO THE DEPARTMENT OF HOMELAND SECURITY REGARDING ITS WORK DEVELOPING A VOLUNTARY PROGRAM UNDER EXECUTIVE ORDER 13636, "IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY" (2014), *available at* http://www.itic.org/dotAsset/3ed86a62-b229-4d43-a12b-766012da4b1f.pdf; *see also* Ann M. Beauchesne, *Administration Sends Cybersecurity Stakeholders a Positive Message: The NIST Framework Should be Voluntary, Flexible, and Collaborative*, U.S. CHAMBER OF COM. (June 11, 2014), http://www.uschamber.com/administration-sends-cybersecurity-stakeholders-positive-message-nist-framework-should-be-voluntary (discussing industry support for NIST Framework and making sure that pre-existing regulations comply); Matt Thomlinson, *The NIST Cybersecurity Framework: A Significant Milestone towards Critical Infrastructure Resiliency*, MICROSOFT CYBER TRUST BLOG (Feb. 13, 2014), http://blogs.technet.com/b/security/archive/2014/02/13/the-nist-cybersecurity-framework-a-significant-milestone-towards-critical-infrastructure-resiliency.aspx (commending NIST for its work on the Framework and confirming Microsoft's compliance with the NIST Framework).

308. PWC, WHY YOU SHOULD ADOPT THE NIST CYBERSECURITY FRAMEWORK 1 (2014), *available at* http://www.pwc.com/en_US/us/increasing-it-effectiveness/publications/assets/adopt-the-nist.pdf.

309. *See* Beauchesne, *supra* note 307 (noting the measures industry members have done to promote cybersecurity since the Framework's issuing).

310. Press Release, ISACA, *supra* note 297.

industry associations, representing energy, information technology, manufacturing, retailing, and other sectors, joined together in June 2014 to applaud the Framework and demonstrate their continued investment in promoting the Framework.[311] For example, industry association Information Technology Industry Council (ITI) explained that it has recently visited Japan and South Korea, sharing with both countries' governments and business leaders "the benefits of a public-private partnership-based approach to developing globally workable cybersecurity policies."[312] Moreover, "ITI highlighted the [F]ramework as an example of an effective policy developed in this manner, reflecting global standards and industry-driven practices."[313]

As an especially global industry—with significant incentives to drive governments toward adopting and implementing global standards, which would ease their compliance and liability fears—information technology leaders may promote the Framework both via industry associations and more directly, with governments themselves. In addition, the insurance industry may also be incentivized to promote the Framework; AIG in the United States has developed a policy that "supports" NIST's Framework, and in the United Kingdom AIG is working with the U.K. government "to see how it can recognise commitments to meet data hygiene standards and enforce cyber security standards."[314] AIG is seeking to support companies by seeking "accord" with government priorities—and like any global industry, the more those government priorities align, the more straightforward such support to industry customers or compliance with government guidelines.[315]

Looking ahead, the legal standards on which U.S. and other lawmakers settle will be important in shaping firms' cybersecurity investments. According to McAfee, "For many companies, security and risk managementdecisions [sic] are based on strict adherence to compliance standards, not on protecting their intellectual capital."[316] Indeed, another McAfee survey found that compliance with regulation is the "key motivator" for security decisions "in Dubai, Germany, Japan, the U.K., and the U.S.;" only in India and China did surveyed companies more often base security decisions on gaining or maintaining competitive advantages.[317] These surveys point to a trend showing that regulations are critical to firms' security investment decisions, even if businesses at times balk at additional regulatory compliance burdens. Consequently, regulatory intervention can play a vital role in enhancing the public good of cybersecurity. But how much is too much?

Survey data from PwC indicate that since 2008, many firms around the world are increasingly unhappy with cybersecurity regulations. As many as 57% of Indian, 58% of U.S., and 72% of Chinese companies agreed that their regulatory

311. *See* Beauchesne, *supra* note 307 (discussing industry support for NIST Framework and making sure that pre-existing regulations comply).

312. *Id.*

313. *Id.*

314. Jamie Bouloux, *A Broader View*, INSIDER Q., Summer 2014, at 38.

315. *Id.*

316. MCAFEE, UNDERGROUND ECONOMIES: INTELLECTUAL CAPITAL AND SENSITIVE CORPORATE DATA NOW THE LATEST CYBERCRIME CURRENCY 16 (2011) [hereinafter MCAFEE, INTELLECTUAL CAPITAL], *available at* http://www.ndia.org/Divisions/Divisions/Cyber/Documents/rp-underground-economies.pdf.

317. MCAFEE, UNSECURED ECONOMIES: PROTECTING VITAL INFORMATION 6 (2009), *available at* http://www.cerias.purdue.edu/assets/pdf/mfe_unsec_econ_pr_rpt_fnl_online_012109.pdf.

environments were becoming "more complex and burdensome."[318] A Symantec report argued that "enterprises are buried with [information technology] compliance efforts," ranging from HIPAA to Sarbanes-Oxley,[319] which, among other things,[320] impose severe fines on companies that are found negligent.[321] Some worry that well-meaning regulations may force companies to focus more on compliance than security,[322] and others disagree about the effectiveness of existing regulations and argue that the onus should be on proponents of greater regulation.[323] In a 2007 Computer Security Institute survey, 25% of respondents "strongly disagree[d]" that Sarbanes-Oxley, for example, has improved their organization's information security, and just 12% "strongly agree[d]" that the regulation had positive effects.[324] Similarly, only a third of respondents to a 2011 McAfee survey said that they "feel that compliance regulations imposed by their home country are very useful and aim at the heart of the problem to protect their corporation's intellectual capital."[325] These findings point to the fact that more needs to be done to fashion effective cybersecurity interventions where needed and to streamline compliance so that the focus is on enhancing cybersecurity and not checking boxes—not only in the United States, but also around the world.

---

318. PRICEWATERHOUSECOOPERS, TRIAL BY FIRE*: WHAT GLOBAL EXECUTIVES EXPECT OF INFORMATION SECURITY—IN THE MIDDLE OF THE WORLD'S WORST ECONOMIC DOWNTURN IN THIRTY YEARS 36 (2010), *available at* http://www.pwc.com/en_GX/gx/information-security-survey/pdf/pwcsurvey2010_report.pdf.

319. SYMANTEC, STATE OF ENTERPRISE SECURITY: 2010, at 12 (2010), *available at* http://www.symantec.com/content/en/us/about/presskits/SES_report_Feb2010.pdf.

320. *See, e.g.*, Health Insurance Portability and Accountability Act of 1996, 18 U.S.C. §§ 669(a), 1347(2) (2012) (imposing penalties for individuals who knowingly and willfully convert to use assets of a health care benefit program or carries or attempts to carry out a plan aimed at defrauding a health care benefit program or otherwise fraudulently obtaining money or property belonging to the health care benefit program in connection with the delivery of benefits); *HIPAA Compliance*, PATIENT PROMPT, http://patientprompt.com/our-technology/compliance-hipaa-pipeda/ (last visited Apr. 3, 2015) (reporting that HIPAA fines can range "up to $250K and/or imprisonment up to 10 years for knowing misuse of individually identifiable health information").

321. *See, e.g.*, Michelle DeBarge & Jody Erdfarb, *US State Supreme Court Expands Potential Negligence Liability for HIPAA Violations*, TERRALEX (Mar. 16, 2015), http://www.terralex.org/publication/ p6cc362bb94/us-state-supreme-court-expands-potential-negligence-liability-for-hipaa-violations (addressing a Connecticut Supreme Court decision that allows plaintiffs on state law negligence claims to use HIPAA as setting the applicable standard of care).

322. *See, e.g.*, Chandra McMahon, *Is Compliance Security? 5 Tips for Balancing the Two*, LOCKHEED MARTIN (Feb. 18, 2015), http://lockheedmartin.com/us/news/features/2015/is-compliance-security.html (noting that in a recent survey of information technology security leaders, the top priority overall was compliance, not security).

323. *See, e.g.*, Jerry Brito & Tate Watkins, *Loving the Cyber Bomb? The Dangers of Threat Inflation in Cybersecurity Policy*, 3 HARV. NAT'L SECURITY J. 39, 82–83 (2011) ("[T]he burden is on proponents of regulation to explain how they determine what is the appropriate level of cybersecurity . . . .").

324. ROBERT RICHARDSON, CSI SURVEY 2007: THE 12TH ANNUAL COMPUTER CRIME AND SECURITY SURVEY 24–25 (2007), http://i.cmpnet.com/v2.gocsi.com/pdf/CSISurvey2007.pdf; *cf. Enhancing and Implementing the Cybersecurity Elements of the Sector-Specific Plans: Joint Hearing before the Subcomm. on Emerging Threats, Cybersecurity & Sci. & Tech. and the Subcomm. on Transp. Sec. & Infrastructure Prot. of the H. Comm. on Homeland Sec.*, 110th Cong. 87 (2007) (statement of Lawrence A. Gordon, Professor, Robert H. Smith School of Business, University of Maryland) (making the empirical case that Sarbanes-Oxley has actually "created a strong incentive for organizations to increase their cybersecurity investments").

325. MCAFEE, INTELLECTUAL CAPITAL, *supra* note 316, at 8.

CONCLUSION

In February 2013, President Obama issued Executive Order 13636: Improving Critical Infrastructure Cybersecurity, which, among other things, called for public-private partnerships with the owners and operators of critical infrastructure to improve cybersecurity information sharing and collaboratively develop approaches to mitigating cyber threats. Specifically, the Executive Order called on the NIST Director "to lead the development of a framework to reduce cyber risks to critical infrastructure."[326] One commentator has argued that the Framework "represents the best efforts of the administration and . . . industry representatives from the 16 critical infrastructure sectors to work together to address a threat which President Obama has called one of the gravest national security dangers the United States faces."[327] But praise has not been universal. Some have cautioned that the Framework does not go far enough in terms of its scope, influence, and initial impact.[328]

Among the less discussed aspects of the Framework is its potential to shape a cybersecurity standard of care for both domestic critical infrastructure firms and potentially the private sector writ globally. Over time, common law liability, coupled with preferential regulatory treatment to organizations that have implemented the Framework, could pressure companies to conform their cybersecurity practices to this "voluntary" Cybersecurity Framework. Whether this development turns out to be beneficial to individual firms in particular and national and international security generally depends on one's views of the seriousness of the cyber threat, the value of the NIST approach, and the ability of the competitive market to identify and implement cybersecurity best practices absent regulatory intervention. This Article begins this conversation by undertaking an introductory examination of the NIST Cybersecurity Framework, focusing on the Framework's evolution, scope, and potential to shape a reasonable standard of cybersecurity care.

Ultimately, we have argued that, while the final impact that the Cybersecurity Framework may have on shaping a standard of cybersecurity care will not be known for some time to come, the Framework could have a significant impact on common law in the United States as well as on what constitutes a cybersecurity standard of care in other jurisdictions, including the United Kingdom, the EU, and India. However, significant barriers in the United States, such as standing concerns, must be overcome for this to take place. Still, business managers, policymakers, and scholars would do well to note the potential impact of the 2014 NIST Framework as cases referencing it begin to move through the courts.

The NIST Framework begins from a very simple, three-step premise: "Determine if your organization even has a formal security program and understand your security posture. Determine what is protected, whether security practices are adaptable and repeatable, and whether they meet your organization's business and mission needs. Identify gaps and develop a road map for improvement."[329] But,

326. Exec. Order No. 13636, 78 Fed. Reg. 33, 11739, 11740–01 (Feb. 19, 2013).

327. Wallace, *supra* note 15, at 2.

328. *See id.* at 16 (indicating that there are gaps in the cybersecurity framework).

329. William Jackson, *Protecting Critical Infrastructure: A New Approach*, INFORMATIONWEEK (Apr. 21, 2014), http://www.informationweek.com/government/cybersecurity/protecting-critical-infrastructure-a-new-approach/d/d-id/1204577?page_number=2.

while the Framework may in many ways read as "common sense,"[330] it is perhaps its simplicity that is also at the heart of its strength since it, even if it accomplishes nothing else, could create a common matrix for managing cyber risk. The NIST Framework is not the whole answer to the multifaceted cybersecurity problem—nor will it alone fashion international due diligence cyber norms. Government regulators can and will also continue efforts to enhance cybersecurity, including for critical infrastructure, through incentivizing the use of such tools as cyber risk insurance, and the market will similarly continue innovating to better manage cyber risk. However, the era of the "voluntary" cybersecurity framework has begun, and its impact will likely be felt in boardrooms and courtrooms across the United States, and perhaps even the world, for many years to come.

330. *Id.*

Cyberwar & International Law Step Zero

KRISTEN E. EICHENSEHR*

SUMMARY

* Visiting Assistant Professor, UCLA School of Law. For helpful comments and conversations, the author is indebted to Ashley Deeks, Richard Re, and participants in the *Texas International Law Journal* Intangible Weaponry & Invisible Enemies Symposium and the Yale Law School Information Society Project Symposium on Cyberwarfare and Killer Robots: How the Law of War Regulates New Technologies. The author also thanks Kevin Whitfield for excellent research assistance and the editors of this *Journal* for bringing the piece to publication. This Article reflects developments through mid-April, when it was finalized for publication.

INTRODUCTION

New technologies pose challenges for law and for international law in particular. For as cumbersome and slow as domestic law appears in many circumstances, developing international law is often even more difficult. Treaties take years to negotiate, and custom may take decades or centuries to solidify. When technology changes faster than law, as it often does, lawyers face the challenge of coping with new technologies using legal rules that were developed before the advent of the new technology and that do not explicitly contemplate it.

The temporal mismatch between technological innovation and development of international law poses a recurring question. In administrative law, the first question courts ask in statutory interpretation cases is whether the agency interpretation at issue is the sort of thing to which courts owe deference under the *Chevron* doctrine.[1] In other words, does the *Chevron* framework apply at all? This is the "*Chevron* step-zero" question.[2] Borrowing this administrative law terminology, this Article focuses on an analogous international law question: Is the new innovation a type of weapon that existing international law can satisfactorily regulate? This is the "international law step-zero" question.

Part I chronicles recent instances in which the "international law step-zero" question has arisen with respect to new technologies and the laws of war, including both the *jus ad bellum* (law governing the resort to force) and the *jus in bello* (law governing the conduct of hostilities).[3] In recent years, states and commentators have repeatedly debated whether the laws of war can and do regulate new technologies. Some have advocated that new technologies should be banned altogether via new treaties because they cannot be regulated effectively by the case-by-case application of existing legal standards. Others have argued that new technologies are not regulated absent some new technology-specific law. Despite the recurring debate over these issues, the answer to the step-zero question often steers a middle course toward rejecting fundamental changes to existing law and regulating new technology through the application of existing law, perhaps with tweaks at the margins to accommodate the peculiar features of new technologies.

In keeping with the theme of this symposium on cyberwar, Part II focuses on cyber weapons as a case study to examine first, why debates continue to arise with respect to the step-zero question, and second, why the frequent answer is the application of existing laws of war.

While noting that the answer to the step-zero question is generally the application of existing laws of war, this Article does not suggest that *no* new law is

1. *See, e.g.*, United States v. Mead Corp., 533 U.S. 218, 227–34 (2001) (holding that tariff classification rulings fail to qualify for *Chevron* deference).

2. Cass R. Sunstein, Chevron *Step Zero*, 92 VA. L. REV. 187, 191 (2006).

3. *See, e.g.*, Derek Jinks, *Protective Parity and the Laws of War*, 79 NOTRE DAME L. REV. 1493, 1493 n.1 (2004) ("The 'law of war' encompasses two distinct bodies of rules: the *jus ad bellum*—rules governing when uses of force are lawful; and the *jus in bello*—rules governing the conduct of war."). I use "law of war" as an umbrella term to encompass both the *jus ad bellum* and the *jus in bello*.

needed for new technologies, but rather that *most* law-of-war rules apply *most* of the time to *most* new technologies,[4] and that any new law specific to a new technology is a comparatively small fraction of the laws of war applicable to that technology. Part III addresses circumstances in which new law may be necessary, again using cyberwar as a case study, and concludes by offering several proposals for cyber-specific additions or amendments to existing laws of war.

I. LAW OF THE (WAR) HORSE?

The advent of new war-fighting technologies has sparked recurring debates about the applicability of existing laws of war. With each new technology, debate resumes about whether the technology is so different from the weapons that preceded it as to make existing law incapable or insufficient as a governing mechanism. Those who say existing law is insufficient advocate some major new law, either a new treaty banning the weapon or a ground-up, weapon-specific redrafting of the *jus ad bellum* or *jus in bello*.

In another context, Judge Frank Easterbrook has criticized the phenomenon of isolating law for particular objects, as captured by the idea of the "law of the horse."[5] Yet, new war-fighting technologies seem to provoke consideration of whether there should be a separate law of war, for example, for nuclear weapons or drones. After the dust settles, the debate frequently resolves in favor of application of existing laws of war, particularly at the level of broad principles, such as proportionality and distinction, with tweaks around the edges as necessary to account for the peculiar characteristics of the new war-fighting technology.

Some weapons, of course, do prompt weapon-specific treaties, specifically treaties that ban use of the weapon entirely.[6] But such bans arguably reinforce existing law of war principles. They represent a determination that a particular type of weapon cannot be used in compliance with, for example, the principles of distinction or proportionality or the prohibition on the infliction of unnecessary suffering.[7] They do not fundamentally alter existing principles in light of new weapons.

This Part chronicles several examples of the international law step-zero question being raised and then resolved through the application of existing law, rather than weapon-specific treaties changing the laws of war or banning the weapon

4. *Cf.* LOUIS HENKIN, HOW NATIONS BEHAVE 47 (2d ed. 1979) ("[A]lmost all nations observe almost all principles of international law and almost all of their obligations almost all of the time." (emphasis omitted)).

5. Frank H. Easterbrook, *Cyberspace and the Law of the Horse*, 1996 U. CHI. LEGAL F. 207, 207. Easterbrook used the law of the horse metaphor to criticize law schools' curricular focus on specialized courses that, in their focus on a single object like a horse, are "doomed to be shallow and to miss unifying principles." *Id.* The metaphor is used here for a different purpose, though some of the risks may be the same. In the curricular context, Lawrence Lessig has pushed back against Easterbrook's criticism of cyberlaw as a "law of the horse" subject. *See generally* Lawrence Lessig, Commentary, *The Law of the Horse: What Cyberlaw Might Teach*, 113 HARV. L. REV. 501 (1999).

6. *See infra* notes 124–1131 (providing examples of treaties that ban particular weapons).

7. *See infra* note 132 and accompanying text.

entirely.[8] The next Part turns to the ongoing debate about cyber conflict as an in-depth case study of the phenomenon.

A. Nuclear Weapons

In 1994, the U.N. General Assembly requested an advisory opinion from the International Court of Justice (ICJ) on whether normal rules of international law apply with respect to the threat or use of nuclear weapons, or whether the nature of nuclear weapons is such that they can never comply with international law.[9] In particular, the General Assembly asked: "Is the threat or use of nuclear weapons in any circumstance permitted under international law?"[10] The question itself set nuclear weapons apart from other types of weapons because international law does permit the use and threat of use of other weapons under certain circumstances.[11] The ICJ took account of "certain unique characteristics of nuclear weapons," including their powerful explosive potential and discharge of radiation,[12] but explained that the prohibition on the threat or use of force contained in Article 2(4) of the U.N. Charter and Article 51's recognition of the right to self-defense "do not refer to specific weapons."[13] The Court explained that Articles 2(4) and 51 "apply to any use of force, regardless of the weapons employed," and the U.N. Charter "neither expressly prohibits, nor permits, the use of any specific weapon."[14] The Court further noted that the customary international law principles of necessity and proportionality apply in cases of self-defense, "whatever the means of force employed."[15]

In considering *jus in bello* (or international humanitarian law (IHL)), the ICJ noted that the "illegality of the use of certain weapons as such . . . is formulated in terms of prohibition,"[16] and "[t]he pattern until now has been for weapons of mass destruction to be declared illegal by specific instruments."[17] Finding no treaty prohibition of nuclear weapons, the Court then considered whether the use of nuclear weapons could comply with existing *jus in bello* in any circumstances.[18] The Court identified as "cardinal principles" the principle of distinction and the prohibition on causing unnecessary suffering to combatants,[19] and concluded that the

8. The Treaty on the Non-Proliferation of Nuclear Weapons, July 1, 1968, 21 U.S.T. 483, 729 U.N.T.S. 161, is a weapon-specific treaty, but it governs proliferation and does not alter existing international law rules governing the use of nuclear weapons. *See* Part I.A *infra*.

9. Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226, para. 1 (July 8).

10. *Id.* para. 20.

11. The use of certain types of weapons, such as chemical and biological weapons, is banned by treaty. *Id.* para. 57. The ICJ examined nuclear weapons as part of the group of weapons that are *not* specifically banned. *Id.*

12. *Id.* para. 35.

13. *Id.* paras. 38–39.

14. *Id.* para. 39.

15. Legality of the Threat or Use of Nuclear Weapons, 1996 I.C.J. 226 para. 41.

16. *Id.* para. 52.

17. *Id.* para. 57.

18. *Id.* para. 74.

19. *Id.* para. 78.

Court shares the view of "the vast majority of States as well as writers" that "there can be no doubt as to the applicability of humanitarian law to nuclear weapons."[20] Citing "the fundamental right of every State to survival, and thus its right to resort to self-defence,"[21] the Court declined to conclude that the use of nuclear weapons could *never* comply with *jus in bello*.[22]

In other words, the Court affirmed that nuclear weapons are subject to the general laws of war, including both the *jus ad bellum* and the *jus in bello*. The unique characteristics of nuclear weapons did not remove them from the ambit of generally applicable international law rules, absent a treaty banning the weapons entirely.[23]

B. Armed Drones

With the use of drones by Israel in the early 2000s and by the United States after the September 11th attacks, questions arose about whether armed drones were lawful weapons.[24] In the face of criticism and debate about the legality of drones, the U.S. government rejected claims that drones are subject to a special legal regime, emphasizing that "the rules that govern targeting do not turn on the type of weapon system used."[25] Rather, the U.S. government took the position that existing law, including the principles of distinction and proportionality, governs operations carried out via "unmanned aerial vehicles," or drones.[26]

---

20. *Id.* paras. 85–86.

21. Legality of the Threat or Use of Nuclear Weapons, 1996 I.C.J. 226 para. 96.

22. *Id.* para. 95.

23. Interestingly, the alternative to application of existing international law rules to nuclear weapons was the possibility that the weapons are so problematic that their use and the threat of their use is banned entirely. *Cf. id.* para. 86 ("None of the statements made before the Court in any way advocated a freedom to use nuclear weapons without regard to humanitarian constraints."); *see also id.* paras. 52–62 (discussing absence of a positive law ban on use of nuclear weapons); *id.* paras 95–96. With respect to other weapons, some would argue that the consequence of determining that existing law does not apply may be leaving the weapon unregulated, as opposed to determining that it is banned altogether.

24. *See, e.g.*, Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions, *Rep. of the Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions: Addendum: Study on Targeted Killings*, paras. 80, 84, Human Rights Council, U.N. Doc. A/HRC/14/24/Add.6 (May 28, 2010) (by Philip Alston) [hereinafter Alston, *Rep. of the Special Rapporteur: Addendum*] (noting concerns that States will "interpret the legal limitations on who can be killed, and under what circumstances, too expansively" because drones eliminate the risk to the attacking State's armed forces and that drone operators may "develop[] a 'Playstation' mentality" due to their distance from the battlefield); Laurie R. Blank, *After "Top Gun": How Drone Strikes Impact the Law of War*, 33 U. PA. J. INT'L L. 675, 683–702 (2012) (providing an overview of debates and arguing that drones as a weapons system comply with existing *jus in bello* requirements); Samuel Issacharoff & Richard H. Pildes, *Targeted Warfare: Individuating Enemy Responsibility*, 88 N.Y.U. L. REV. 1521, 1570–78 (2013) (rebutting arguments that drones are legally problematic because they enable targeting at a distance and, by insulating operators from risk, make war too easy); Murray Wardrop, *Unmanned Drones Could Be Banned, Says Senior Judge*, TELEGRAPH, July 6, 2009, http://www.telegraph.co.uk/news/uknews/ defence/5755446/Unmanned-drones-could-be-banned-says-senior-judge.html (quoting Lord Bingham, a retired senior law lord, suggesting that armed drones, like landmines and cluster munitions, could be banned).

25. Harold Hongju Koh, Legal Adviser, U.S. Dep't of State, The Obama Administration and International Law, Remarks at the Annual Meeting of the American Society of International Law (Mar. 25, 2010), *available at* http://www.state.gov/s/l/releases/remarks/139119.htm.

26. *Id.*

Similarly, Philip Alston, then the U.N. Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions, issued a report that, although critical of targeted killings for other reasons, recognized that "a missile fired from a drone is no different from any other commonly used weapon, including a gun fired by a soldier or a helicopter or gunship that fires missiles. The critical legal question is the same for each weapon: whether its specific use complies with IHL."[27]

Looking back over the last decade, the drones debate is now largely settled in favor of application of existing law,[28] though debates remain about how that law applies in particular circumstances.[29] As another U.N. Special Rapporteur acknowledged in 2013, "[d]rones, it can safely be said, are here to stay."[30]

C. Lethal Autonomous Weapons Systems

Similar debates to those about nuclear weapons and drones are also beginning with respect to lethal autonomous weapon systems (LAWS), or, as some have dubbed them, "killer robots."[31] In fact, a recent U.N. report contrasted the legal debate over drones and autonomous weapons, noting that as of 2013, "[t]here is broad agreement that drones themselves are not illegal weapons. This is not the case . . . with lethal autonomous robots."[32] Robotics expert P.W. Singer has dubbed the legal uncertainty surrounding robots "unmanned legal confusion,"[33] and Human Rights Watch has proposed an international treaty to prohibit "fully autonomous weapons."[34]

---

27. Alston, *Rep. of the Special Rapporteur: Addendum*, *supra* note 24, para. 79.

28. Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions, *Rep. of the Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions*, para. 19 (2013), *transmitted by Note of the Secretary-General*, U.N. Doc. A/68/382 (Sept. 13, 2013) (by Christof Heyns) [hereinafter Heyns, *Rep. of the Special Rapporteur*] ("A decade or so ago, the use of armed drones was relatively novel and untested; their human impact and further technological development were hard to predict, and a full discussion of the proper application of the international legal framework had yet to emerge. A vast body of academic and advocacy literature has now developed . . . ."); Michael N. Schmitt, *Narrowing the International Law Divide: The Drone Debate Matures*, 39 YALE J. INT'L L. ONLINE 1, 2 (2014) (noting, based on U.N. and human rights group reports, that "substantial agreement now exists between key parties," including states and IHL experts as well as the human rights community, about "the legal framework for drone operations" and declaring that this agreement represents "a sea change in the nature of the debate over drones").

29. *See* Blank, *supra* note 24, at 716–17 ("Use of armed drones continues to raise serious questions about the numbers and nature of civilian casualties, but these questions stem primarily from the procedures for selecting targets and approving attacks, not from the nature and capabilities of drones themselves." (footnote omitted)).

30. Heyns, *Rep. of the Special Rapporteur*, *supra* note 28, para. 12; *see also id.* para. 104 ("The established international legal framework for the use of force (international human rights law, international humanitarian law and inter-State force) should be regarded as setting forth an adequate framework for the use of armed drones." (emphasis omitted)).

31. *See Killer Robots*, HUM. RTS. WATCH, http://www.hrw.org/topic/arms/killer-robots (last visited Apr. 28, 2015); CAMPAIGN TO STOP KILLER ROBOTS, http://www.stopkillerrobots.org/ (last visited Apr. 28, 2015).

32. Heyns, *Rep. of the Special Rapporteur*, *supra* note 28, para. 13.

33. P.W. SINGER, WIRED FOR WAR 383 (2009).

34. HUM. RTS. WATCH, LOSING HUMANITY: THE CASE AGAINST KILLER ROBOTS 46 (2012), *available at* http://www.hrw.org/sites/default/files/reports/arms1112_ForUpload.pdf ("States should preemptively ban fully autonomous weapons because of the threat these kinds of robots would pose to

As technology progresses, States and commentators are beginning to devote serious attention to the legal and other issues surrounding LAWS. In May 2014, the United Nations held its first meeting on LAWS in conjunction with the Convention on Certain Conventional Weapons.[35] As a follow-on, a group of governmental and non-governmental experts convened in April 2015 to continue discussions of legal and other issues regarding LAWS, including the challenges they pose for *jus in bello*.[36] Scholars also continue to examine whether and how LAWS can comply with the laws of war.[37]

The next Part situates cyberwar in this timeline of step-zero debates and delves into why the debate—and the resolution—has recurred.

II. ZEROING IN

A. Cyberwar and the Step-Zero Question

The debates in recent years regarding the international law applicable to cyberwar provide an apt case study to consider why such debates recur and why the answer has generally been the application of existing law.

Cyberspace and the Internet began as a government-sponsored academic research network.[38] In the 1990s, the Internet began to spread to the public and take on the first signs of the prominence it now occupies in daily life. At that time, some Internet proponents raised a serious "step-zero" question about whether *any* law, not just international law, could or should reach the Internet. John Perry Barlow of the Electronic Frontier Foundation issued a "Declaration of Independence of Cyberspace," which declared:

---

civilians during times of war.").

35. *See* Ishaan Tharoor, *Should the World Kill Killer Robots Before It's Too Late?*, WASH. POST (May 12, 2014), http://www.washingtonpost.com/blogs/worldviews/wp/2014/05/12/should-the-world-kill-killer-robots-before-its-too-late/; *UN Meeting Targets "Killer Robots"*, UN NEWS CENTRE (May 14, 2014), http://www.un.org/apps/news/story.asp?NewsID=47794#.U9l23mMhUsQ.

36. The meeting website has a useful compilation of statements by governments, as well as NGO and academic experts. *See 2015 Meeting of Experts on LAWS*, U.N. OFF. GENEVA, http://www.unog.ch/80256EE600585943/%28httpPages%29/6CE049BE22EC75A2C1257C8D00513E26?OpenDocument (last visited Apr. 28, 2015).

37. *See, e.g.*, Kenneth Anderson & Matthew Waxman, LAW AND ETHICS FOR AUTONOMOUS WEAPON SYSTEMS: WHY A BAN WON'T WORK AND HOW THE LAWS OF WAR CAN (2013), *available at* http://www.hoover.org/research/law-and-ethics-autonomous-weapon-systems-why-ban-wont-work-and-how-laws-war-can (assessing legal arguments against autonomous weapons); Rebecca Crootof, *The Killer Robots Are Here: Legal and Policy Implications*, 36 CARDOZO L. REV. (forthcoming 2015), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2534567 (analyzing autonomous weapons' compatibility with distinction and proportionality); Marco Sassóli, *Autonomous Weapons and International Humanitarian Law: Advantages, Open Technical Questions and Legal Issues to be Clarified*, 90 INT'L L. STUD. 308 (2014) (discussing *jus in bello* questions related to autonomous weapons); Patrick Lin, *Do Killer Robots Violate Human Rights?*, ATLANTIC, Apr. 20, 2015, http://www.theatlantic.com/technology/archive/2015/04/do-killer-robots-violate-human-rights/390033/(discussing the Martens Clause).

38. For a brief overview of the development of the Internet, see P.W. SINGER & ALLAN FRIEDMAN, CYBERSECURITY AND CYBERWAR: WHAT EVERYONE NEEDS TO KNOW 16–20 (2014).

> Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of [the] Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather.[39]

The cry of independence from law and government was carried forward in academic circles as well. In an influential article, David Johnson and David Post argued that the Internet, by "cut[ting] across territorial borders, creat[es] a new realm of human activity and undermin[es] the feasibility—and legitimacy—of laws based on geographic borders."[40] They argued that instead of the existing territorial sovereignty model, cyberspace should be governed by rules determined by its users, and that so long as such rules do not "fundamentally impinge upon the vital interests of others who never visit this new space, then the law of sovereigns in the physical world should defer to this new form of self-government."[41]

This view that cyberspace was and should be beyond the reach of territorial sovereigns provoked immediate push-back. Academics argued that governments could and should regulate conduct on the Internet.[42] They noted that the physical hardware underlying the Internet is located within States' territory, and that a State can legitimately regulate technology within its borders, people within its borders, and the "local effects of extraterritorial acts."[43]

Governments' efforts to regulate cyberspace through domestic law were swift and determinative. States embraced their ability to regulate cyberspace through both existing laws and new, Internet-tailored laws,[44] and contrary to the wishes of the early Internet partisans, cyberspace did not evolve as a law-free zone.[45]

---

39. John Perry Barlow, *A Declaration of the Independence of Cyberspace*, ELECTRONIC FRONTIER FOUND. (Feb. 8, 1996), http://w2.eff.org/Censorship/Internet_censorship_bills/barlow_0296.declaration; *see also id.* ("We must declare our virtual selves immune to your sovereignty, even as we continue to consent to your rule over our bodies.").

40. David R. Johnson & David Post, *Law and Borders—The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367, 1367 (1996); *see also id.* at 1375 ("The rise of an electronic medium that disregards geographical boundaries throws the law into disarray by creating entirely new phenomena that need to become the subject of clear legal rules but that cannot be governed, satisfactorily, by any current territorially based sovereign.").

41. *Id.* at 1393.

42. *See, e.g.*, Jack L. Goldsmith, *The Internet and the Abiding Significance of Territorial Sovereignty*, 5 IND. J. GLOBAL LEGAL STUD. 475, 475 (1998) ("[T]erritorial regulation of the Internet is no less feasible and no less legitimate than territorial regulation of non-Internet transactions."); Timothy S. Wu, Note, *Cyberspace Sovereignty?—The Internet and the International System*, 10 HARV. J.L. & TECH. 647, 649–56 (1997) (arguing that states have the capacity to regulate the Internet).

43. Goldsmith, *supra* note 42, at 476–77; *see also* Wu, *supra* note 42, at 651 ("By exercising control over the physical components required for Internet access, the state can regulate cyberspace.").

44. In the United States, for example, federal statutes specifically addressing Internet and computer-related issues include the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (2012), the Electronic Communications Privacy Act, 18 U.S.C. §§ 2510–22 (2012), and the Unlawful Internet Gambling Enforcement Act, 31 U.S.C. §§ 5361–67 (2012). U.S. states have also adopted cybercrime statutes, *see, e.g.*, CAL. PENAL CODE § 502 (West, Westlaw through 2014 legislation) ("Unauthorized access to computers, computer systems and computer data"); 18 PA. CONS. STAT. ANN. § 7616 (West, Westlaw through 2014 legislation) ("Distribution of computer virus"); WASH. REV. CODE ANN. § 9A.52.110 (West, Westlaw through 2014 legislation and initiative measures) ("Computer Trespass"), as have many foreign countries, *see, e.g.*, *Cybercrime Legislation – Country Profiles*, COUNCIL OF EUR., http://www.coe.int/t/DGHL/cooperation/

With the applicability and reach of domestic law to the Internet now clear, the debate has shifted to the international realm, where countries and commentators debate whether cyberspace is or can be regulated with existing law or whether new law is needed. At the level of governments, many countries agree that cyberspace is a domain of military activity,[46] but a robust debate is ongoing about whether existing international laws, and particularly the laws of war, apply or are sufficient or whether entirely new law is needed.[47]

Two camps have coalesced. On one side, the United States and its allies have argued that existing laws regarding the use of force and conduct of hostilities apply to cyberspace.[48] For example, the 2011 U.S. International Strategy for Cyberspace advocates the development of norms for "state conduct in cyberspace," but emphasizes that such development "does not require a reinvention of customary

---

economiccrime/cybercrime/Documents/CountryProfiles/default_en.asp (last visited Apr. 28, 2015).

45. To be sure, there remain many challenging second-order questions about how the Internet and cyberspace are regulated as a matter of domestic law. In the United States, for example, unresolved questions surround the scope of courts' authority to exercise personal jurisdiction over companies for business conducted over the Internet. *Compare* Zippo Mfg. Co. v. Zippo Dot Com, Inc., 952 F. Supp. 1119, 1124 (W.D. Pa. 1997) (proposing a "sliding scale" for specific personal jurisdiction arising from business conducted over the Internet), *with* Oldfield v. Pueblo de Bahio Lora, S.A., 558 F.3d 1210, 1219 n.26 (11th Cir. 2009) (noting some Circuits' acceptance of *Zippo*, but expressing skepticism and noting academic criticism). Courts have also divided over the proper scope of the Computer Fraud and Abuse Act. *See, e.g.*, WEC Carolina Energy Solutions LLC v. Miller, 687 F.3d 199, 203 (4th Cir. 2012) (providing overview of disagreement between circuit courts).

46. Countries that view cyberspace as a military domain include, for example, the United States, U.S. DEP'T OF DEF., DEPARTMENT OF DEFENSE STRATEGY FOR OPERATING IN CYBERSPACE 5 (2011), *available at* http://www.defense.gov/news/d20110714cyber.pdf; China, DEP'T OF DEF., ANNUAL REPORT TO CONGRESS: MILITARY AND SECURITY DEVELOPMENTS INVOLVING THE PEOPLE'S REPUBLIC OF CHINA 2013, at 37 (2013) [hereinafter MILITARY AND SECURITY DEVELOPMENTS INVOLVING CHINA], *available at* http://www.defense.gov/pubs/2013_china_report_final.pdf; the United Kingdom, Tom Espiner, *UK Launches Dedicated Cybersecurity Agency*, ZDNET (June 25, 2009), http://www.zdnet.com/uk-launches-dedicated-cybersecurity-agency-3039667231/; Iran, David E. Sanger, *Obama Order Sped Up Wave of Cyberattacks Against Iran*, N.Y. TIMES, June 1, 2012, at A1 (noting that Iran established a military cyber unit in 2011); and Israel, Hadas Duvdevani, *Internet Has Become a Real Battlefield*, ISRAEL DEF. FORCES (Jan. 8, 2012), http://www.idf.il/1086-14464-EN/Dover.aspx. A 2011 study reported that 33 states "include cyberwarfare in their military planning and organization," and 12 states have established or plan to establish "military cyberwarfare organizations" by 2012. JAMES A. LEWIS & KATRINA TIMLIN, CTR. FOR STRATEGIC & INT'L STUDIES, CYBERSECURITY AND CYBERWARFARE: PRELIMINARY ASSESSMENT OF NATIONAL DOCTRINE AND ORGANIZATION 3–4 (2011), *available at* http://www.unidir.org/programmes/emerging-security-threats/perspectives-on-cyber-war-legal-frameworks-and-transparency-and-confidence-building.

47. For additional discussion of the debate over the applicability of international law to cyberspace, see Kristen E. Eichensehr, *The Cyber-Law of Nations*, 103 GEO. L.J. 317, 328–35 (2015).

48. *See, e.g.*, AUSTL. GOV'T, DEP'T OF DEF., DEFENCE WHITE PAPER 2013 para. 2.89 (2013), *available at* http://www.defence.gov.au/whitepaper/2013/docs/WP_2013_web.pdf ("Australia believes that the existing framework of international law, including the UN Charter and international humanitarian law, applies to cyberspace."); JAPAN INFO. SEC. POLICY COUNCIL, INTERNATIONAL STRATEGY ON CYBERSECURITY COOPERATION, para. 4.3.2 (2013), *available at* http://www.nisc.go.jp/active/kihon/pdf/InternationalStrategyonCybersecurityCooperation_e.pdf ("Japan is of the view that existing international law, including the U.N. Charter and international humanitarian law, naturally applies to acts in cyberspace."); Press Release, NATO, Wales Summit Declaration, para. 72 (Sept. 5, 2014), http://www.nato.int/cps/ic/natohq/official_texts_112964.htm (declaring that "international law, including international humanitarian law and the UN Charter, applies in cyberspace").

international law, nor does it render existing international norms obsolete."[49] Rather, "[l]ong-standing international norms guiding state behavior—in times of peace and conflict—also apply in cyberspace."[50] The U.S. Strategy similarly emphasizes that "hostile acts in cyberspace," like other hostile actions, can justify action in self-defense and that defensive actions must be undertaken "consistent with applicable international law."[51] Subsequent statements by U.S. government officials have reiterated the U.S. view that "international law principles do apply in cyberspace," and that "the law of armed conflict applies to regulate the use of cyber tools in hostilities, just as it does other tools."[52]

However, the applicability of existing international law to cyberspace is not settled.[53] In particular, China has declined to agree that existing IHL applies to cyberspace.[54] In September 2011, several months after the United States released its International Strategy for Cyberspace declaring the applicability of existing international law, China, Russia, Tajikistan, and Uzbekistan proposed a draft treaty, the "International Code of Conduct for Information Security."[55] The Code would have required States to "comply with the Charter of the United Nations,"[56] but it did not otherwise address existing international law, including *jus in bello*. Instead, it proposed a new provision pursuant to which States would commit "[n]ot to use information and communications technologies, including networks, to carry out hostile activities or acts of aggression, pose threats to international peace and security or proliferate information weapons or related technologies."[57] The proposal of a new treaty and lack of reference to existing international laws suggested that the proposing countries disagreed with the U.S. view regarding the applicability of existing *jus in bello*.

---

49. EXEC. OFFICE OF THE PRESIDENT OF THE U.S., INTERNATIONAL STRATEGY FOR CYBERSPACE: PROSPERITY, SECURITY, AND OPENNESS IN A NETWORKED WORLD 9 (2011), *available at* http://www.whitehouse.gov/ sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

50. *Id.*

51. *Id.* at 14; *see also* EXEC. OFFICE OF THE PRESIDENT OF THE U.S., NATIONAL SECURITY STRATEGY 13 (2015), *available at* https://www.whitehouse.gov/sites/default/files/docs/2015_national_security_strategy.pdf (declaring that the United States will defend itself "consistent with U.S. and international law, against cyber attacks").

52. Harold Hongju Koh, Legal Adviser, U.S. Dep't of State, International Law in Cyberspace, Remarks to the USCYBERCOM Inter-Agency Legal Conference, Ft. Meade, MD (Sept. 18, 2012), *in* 54 HARV. INT'L L.J. ONLINE 1, 3–4 (2012) [hereinafter Koh, Remarks to USCYBERCOM Conference]; *see also* Rebecca Ingber, *Interpretation Catalysts and Executive Branch Legal Decisionmaking*, 38 YALE J. INT'L L. 359, 402 (2013) (explaining that speeches like the one cited undergo interagency clearance and are "generally taken to be the coordinated view[] of the U.S. government as a whole").

53. *See* Koh, Remarks to USCYBERCOM Conference, *supra* note 52, at 3 ("At least one country has questioned whether existing bodies of international law apply to the cutting edge issues presented by the internet. Some have also said that existing international law is not up to the task, and that we need entirely new treaties to impose a unique set of rules on cyberspace.").

54. MILITARY AND SECURITY DEVELOPMENTS INVOLVING CHINA, *supra* note 46, at 37 ("Although China has not yet agreed with the U.S. position that existing mechanisms, such as international humanitarian law, apply in cyberspace, Beijing's thinking continues to evolve.").

55. Permanent Representatives of China, the Russian Federation, Tajikistan, and Uzbekistan to the United Nations, Letter Dated 12 Sept. 2011 to the Secretary General, annex, U.N. Doc. A/66/359 (Sept. 14, 2011), *available at* http://www.rusemb.org.uk/data/doc/internationalcodeeng.pdf.

56. *Id.* annex (a).

57. *Id.* annex (b).

In what appeared to be a significant move away from their earlier reticence about the applicability of international law to cyberspace, China and Russia, along with the United States, Australia, France, Germany, and nine other countries, joined consensus in June 2013 in the U.N. Group of Governmental Experts (GGE) in the field of Information and Telecommunications in the Context of International Security on the principle that "[i]nternational law, and in particular the Charter of the United Nations," applies in cyberspace.[58] Although confirming the applicability of the U.N. Charter, the consensus statement leaves much unclear, including whether China, Russia, and others agree or are moving toward agreement that *jus in bello* applies to cyberspace.

Moreover, in January 2015, China and Russia may have backtracked from even the general statement in the 2013 GGE report. Russia and China, along with Kazakhstan, Kyrgyzstan, Tajikistan, and Uzbekistan, sent a revised draft International Code of Conduct for Information Security to U.N. Secretary-General Ban Ki-Moon.[59] The revised draft, like the initial draft, would obligate States to comply with the U.N. Charter,[60] but it does not reference the GGE report's statement that international law applies in cyberspace. The revised draft instead references only an earlier paragraph of the GGE report that discusses "norms derived from existing international law" and the possibility of developing additional norms "over time."[61] In light of the revised draft Code, the proposing States' position on the applicability of existing international law to cyberspace remains unclear.[62]

Similar debates about the applicability of existing laws of war to conflict-related activity in cyberspace have occurred among scholars and commentators. Some have

---

58. Grp. of Governmental Experts on Devs. in the Field of Info. and Telecomms. in the Context of Int'l Sec., *Rep. of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, para. 19 (2013), *transmitted by Note of the Secretary-General*, U.N. Doc. A/68/98* (June 24, 2013) [hereinafter *U.N. GGE Report*], *available at* http://undocs.org/A/68/98; *see also* Press Statement, U.S. Dep't of State, Statement on Consensus Achieved by the UN Group of Governmental Experts on Cyber Issues (June 7, 2013), *available at* http://www.state.gov/r/pa/prs/ps/2013/06/210418.htm (noting that the United States "is pleased to join consensus to affirm the applicability of international law to cyberspace").

59. Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations, Letter Dated 9 Jan. 2015 to the Secretary-General, U.N. Doc. A/69/723, *available at* http://undocs.org/A/69/723.

60. *Id.* at 4 (para. 2(1)).

61. *Id.* (citing *U.N. GGE report*, *supra* note 58, para. 16); *U.N. GGE Report*, *supra* note 58, para. 16.

62. For additional details on the revised International Code of Conduct, see Kristen Eichensehr, *International Cyber Governance: Engagement Without Agreement?*, JUST SECURITY (Feb. 2, 2015, 9:01 AM), http://justsecurity.org/19599/international-cyber-governance-engagement-agreement/. Moreover, at the April 2015 Global Conference on Cyberspace, China's Ambassador to the Netherlands, Chen Xu, again refrained from agreeing that existing international law, especially *jus in bello*, applies to cyberspace. Instead, he stated only that that U.N. Charter is "relevant to [the] behavior of states in cyberspace," as are "universally recognized fundamental norms and principles enshrined" in the Charter, "such as sovereign equality, non-intervention of domestic affairs, no threat or use of force as well as peaceful settlement of international disputes." H.E. Chen Xu, *International Peace and Security in the Context of Cyberspace*, EMBASSY OF THE PEOPLE'S REPUBLIC OF CHINA IN THE KINGDOM OF THE NETHERLANDS (Apr. 16, 2015), http://nl.china-embassy.org/eng/xwdt/t1255769.htm.

argued that existing law is sufficient, while others have argued for new and different rules and new treaties to embody them.[63]

***

Decades after the establishment of the Internet and years after the establishment of military units dedicated to operations in cyberspace, the applicability of existing laws of war—the step-zero question—remains unsettled. The next Part examines why the step-zero question recurs with respect to the laws of war, and Part II.C then turns to possible explanations for the repeated answer that existing law applies to new technologies.

B. The Persistence of the Step-Zero Question

Several factors may contribute to the recurring question about whether existing laws of war apply to new developments in war-fighting.

1. Nature of International Law as a Backdrop

Although cyberspace provoked even domestic law step-zero debates,[64] step-zero questions seem to occur more frequently in the international sphere. The nature of international law itself may facilitate the international law step-zero question.

First, international law has traditionally operated at the level of sovereign States,[65] and the independence of sovereigns engendered a strong tradition that States are bound only by international law to which they consent.[66] The consent-based nature of international obligations is particularly clear with respect to treaties, which bind only states that sign and ratify them.[67] It is also true to a somewhat more limited extent with respect to customary international law, which develops when there is uniform state practice undertaken out of a sense of legal obligation (*opinio*

63. *See, e.g.*, Oona A. Hathaway et al., *The Law of Cyber-Attack*, 100 CALIF. L. REV. 817, 880–82 (2012) (proposing a new "Cyber-Attack Treaty" to provide clarity on, *inter alia*, the definition of cyber war and "when cyber-attacks amount to an armed conflict that warrants self-defense"); Eric Talbot Jensen, *The Future of the Law of Armed Conflict: Ostriches, Butterflies, and Nanobots*, 35 MICH. J. INT'L L. 253, 263–64 & nn.40–41 (2014) (noting disagreements between some who argue that "existing law is sufficiently flexible to respond to new technologies such as cyber capabilities," and others who "argue that a whole new set of rules should be written to provide proper guidance").

64. *See supra* notes 38–45.

65. In recent decades, international law has also reached into States to individuals, for example, through recognizing individual human rights and holding individuals accountable under international criminal law. *See* JAMES CRAWFORD, BROWNLIE'S PRINCIPLES OF PUBLIC INTERNATIONAL LAW 16–17 (8th ed. 2012) ("At a fundamental level, the power structures within the international system are such that sovereignty and statehood remain the basic units of currency," but "[i]t is no longer possible to deny that individuals may have rights and duties in international law . . . .").

66. *See id.* at 9 ("The apparent paradox of how law could operate between sovereigns is resolved by the priority given to consent in the formation of legal obligation and the role of co-operation in interstate affairs—combined with the insight that sovereignty includes the capacity to make commitments not merely temporary in character.").

67. *See* RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW § 102 cmt. f (1987) ("An international agreement creates obligations binding between the parties under international law.").

juris).[68] Customary international law binds all States with no requirement that individual states consent to be bound, but it incorporates an opt-out mechanism whereby States can exempt themselves by persistently objecting to custom as it develops.[69] The tradition of requiring state consent (or at least non-objection) to international law predisposes the international legal community to approach new issues from the ground up: When a new issue arises, the question is whether international law addresses the issue, because if there is no evidence that it does, then it does not.[70] The foundation of international law in state consent triggers a perennial examination of the applicability and scope of coverage of international law that provides a framework for and nudge toward consideration of the possibility that no international law exists to address a particular issue.[71]

Second, the practice-based nature of customary international law may make it particularly susceptible to reconsideration. In the international sphere, the sovereigns that make customary international law through their state practice are the same actors that enforce the law that they develop through repeated interactions with other sovereigns.[72] In the absence of an external adjudicator of law's applicability—the role played in the domestic sphere by courts, but left mostly vacant at the international level[73]—sovereigns together can decide that existing law is inapplicable, that new law is needed, or that no law should apply. In other words, the law makers at the international level (sovereign States) are also the adjudicators of law's applicability, and they may decide that law does not apply. With no external check on sovereigns' behavior besides the views of other sovereigns,[74] States may feel freer to ask and answer the step-zero question at the international level than executive branches at the domestic level, who are more frequently subject to judicial review.

---

68. *See id.* § 102(2); CRAWFORD, *supra* note 65, at 24–27.

69. *See* RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW § 102 cmt. d (1987); CRAWFORD, *supra* note 65, at 28; *see also* Curtis A. Bradley & Mitu Gulati, *Withdrawing from International Custom*, 120 YALE L.J. 202, 233–39 (2010) (tracking the development of the "persistent objector" doctrine).

70. S.S. "Lotus" (Fr. v. Turk.), 1927 P.C.I.J. (ser. A) No. 10, at 18–19 (Sept. 7) ("Restrictions upon the independence of States cannot . . . be presumed.").

71. Similar examinations occur rarely, but not never, within domestic law. *See supra* notes 38–45.

72. *See* W. Michael Reisman, *Assessing Claims to Revise the Laws of War*, 97 AM. J. INT'L L. 82, 82 (2003) (describing a "ceaseless dialectic of international law" whereby "one state claims from others acquiescence in a new practice," and "[i]nsofar as that new practice is accepted in whole or in part, the practice becomes part of the law").

73. *See* Jack Goldsmith & Daryl Levinson, *Law for States: International Law, Constitutional Law, Public Law*, 122 HARV. L. REV. 1791, 1807 (2009) (explaining that although there are international courts "of various kinds in operation, their jurisdictions are narrow and segmented, creating a patchwork of adjudicative authority" that "includes both gaping holes and areas of uncoordinated overlap," leaving "many matters—immigration, war, human rights, and so on—over which international courts have little or no authority").

74. This is not to say that the views of other States and States' "acculturation" into the international legal system exert no pressure; far from it. *See* RYAN GOODMAN & DEREK JINKS, SOCIALIZING STATES: PROMOTING HUMAN RIGHTS THROUGH INTERNATIONAL LAW 38–52 (2013).

2. Reasons for Recurrence

While the two characteristics of international law just discussed may help to explain why the step-zero question occurs in international law, more specific considerations shed light on why the step-zero question recurs particularly frequently with respect to the laws of war. Several possible reasons may explain the prevalence of the step-zero question with respect to cyberwar and to new military technology more generally.

The frequency of the step-zero question is likely driven at least in part by the frequency with which new weapons are developed. States invest heavily in creating new weapons,[75] and in recent decades, they have developed new weapons systems that operate in qualitatively different ways than their predecessors. For example, some viewed military use of armed drones as qualitatively different from past technologies because drone operators engage in combat from secure locations far from the battlefield, including from bases within the United States.[76] In the cyberwar context, commentators have questioned how even to define cyber weapons, which consist of computer code.[77] The frequent development of new technologies that are perceived as qualitatively distinguishable from earlier weapons motivates reconsideration of whether laws developed and adopted prior to the technology's arrival are up to the task of addressing qualitatively different weapons. The perceived discrete nature of new weapons sparks the question of whether a discrete category of law is necessary. This is the "law of the horse" phenomenon discussed above.[78]

The frequency of the step-zero question may also stem not just from the qualitatively different nature of new weapons themselves, but from the frequency

75. *See, e.g.*, OFFICE OF THE SEC'Y OF DEF., ANNUAL REPORT TO CONGRESS: MILITARY AND SECURITY DEVELOPMENTS INVOLVING THE PEOPLE'S REPUBLIC OF CHINA 2014, at ii (2014), *available at* http://www.defense.gov/pubs/2014_DoD_China_Report.pdf (reporting that in 2013, China "announced a 5.7 percent increase in its annual military budget to $119.5 billion"); Barton Gellman & Ellen Nakashima, *U.S. Spy Agencies Mounted 231 Offensive Cyber-Operations in 2011, Documents Show*, WASH. POST, Aug. 30, 2013, http://www.washingtonpost.com/world/national-security/us-spy-agencies-mounted-231-offensive-cyber-operations-in-2011-documents-show/2013/08/30/d090a6ae-119e-11e3-b4cb-fd7ce041d814_story.html (detailing U.S. budget for cyber operations); Phil Stewart, *Chinese Military Spending Exceeds $145 Billion, Drones Advanced: U.S.*, REUTERS (June 5, 2014), http://www.reuters.com/article/2014/06/05/us-usa-china-military-idUSKBN0EG2XK20140605 ("Chinese military spending exceeded $145 billion last year as it advanced a program modernizing an arsenal of drones, warships, jets, missiles and cyber weapons, the Pentagon said on Thursday, offering a far higher figure than Beijing's official tally.").

76. *See, e.g.*, Elisabeth Bumiller, *A Day Job Waiting for a Kill Shot a World Away*, N.Y. TIMES, July 29, 2012, http://www.nytimes.com/2012/07/30/us/drone-pilots-waiting-for-a-kill-shot-7000-miles-away.html?pagewanted=all&_r=0; Jane Mayer, *The Predator War: What Are the Risks of the C.I.A.'s Covert Drone Program?*, NEW YORKER, Oct. 26, 2009, http://www.newyorker.com/magazine/2009/10/26/ the-predator-war; *see also* sources cited *supra* note 24.

77. *See, e.g.*, Louise Arimatsu, *A Treaty for Governing Cyber-Weapons: Potential Benefits and Practical Limitations*, *in* 2012 4TH INTERNATIONAL CONFERENCE ON CYBER CONFLICT PROCEEDINGS 91, 97–98 (C. Czosseck et al. eds., 2012), *available at* https://ccdcoe.org/cycon/2012/proceedings/d3r1s6_arimatsu.pdf (discussing possible definitions of "cyber weapon"); Paul Rosenzweig, *Problems with Cyber Arms Control*, LAWFARE (Feb. 26, 2015, 3:17 PM), http://www.lawfareblog.com/2015/02/problems-with-cyber-arms-control/ ("One will scour the literature for a definition [of cyber weapon] – right now we know it when we see it. But that means we only know it when it is used . . . .").

78. *See supra* note 5 and accompanying text.

with which new weapons produce new and different effects from their predecessors or uncertainty about their effects.[79] Uncertainty about how to conceptualize or predict a new weapon's effects provokes questions about whether the technology is or could be used in a way that is compatible with *jus in bello* requirements, like proportionality and distinction.

The frequency of the step-zero question is also driven by the fact that several distinct groups have reasons and mechanisms to raise the question.

The first group is military officials charged with evaluating the lawfulness of new weapons under existing international law.[80] The weapons review process necessarily raises the step-zero question as militaries considering new weapons ask whether use of the new weapon can comply with *jus in bello* restrictions. For military officials whose deployment of weapons has serious consequences—for their targets and, in light of possible criminal liability for law of war violations, for themselves—the importance of the step-zero question and the need for a certain answer may be particularly salient.

A second group with an incentive to ask the step-zero question is states writ large (as opposed to military officials engaged in weapons review), particularly if States are dissatisfied with the allocation of power under existing laws of war. If, for example, a State dislikes an existing rule of international law, the State may exploit the opportunity provided by the advent of a new technology to attempt to reopen an otherwise settled debate or to try to change the existing rule going forward as applied to the new technology. States might also focus more specifically on their relative capacities with respect to a new technology. For example, a State that perceives itself to be dominant in cyber military capabilities might ask the step-zero question in order to advocate for a regime that would be more permissive than application of existing rules in order to exploit its dominance. Conversely, a State that is comparatively weak in cyber capabilities might ask the step-zero question in order to advocate for a more restrictive set of rules than application of existing law would suggest or perhaps for an outright ban on cyber weapons.

A third group that routinely asks the step-zero question is non-governmental organizations (NGOs), particularly those with a human rights-related mandate. As noted above, Human Rights Watch has analyzed the step-zero question with respect to "killer robots" and supports a treaty banning such weapons on the grounds that

79. For example, commentators still struggle with how to categorize and regulate cyber technologies that may be designed to cause chaos and economic harm, but no physical destruction (e.g., cyber technologies that could alter or wipe out financial records). *See* TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE r. 13 cmt. 9 (Michael N. Schmitt ed., 2013) [hereinafter TALLINN MANUAL], *available at* https://ccdcoe.org/tallinn-manual.html.

80. States parties to Additional Protocol I to the Geneva Conventions are required to engage in weapons review. Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I), art. 36, June 8, 1977, 1125 U.N.T.S. 3. According to the *Tallinn Manual*, the weapons review obligation "has matured through State practice into customary international law," TALLINN MANUAL r. 48 cmt. 2, as evidenced by the fact that non-parties to Additional Protocol I, including the United States, also engage in weapons review, *see* DEP'T OF THE NAVY ET AL., NWP 1-14M/MCWP 5-12.1/COMDTPUB P5800.7A, THE COMMANDER'S HANDBOOK ON THE LAW OF NAVAL OPERATIONS 5.3.4 (2007), *available at* https://www.usnwc.edu/getattachment/a9b8e92d-2c8d-4779-9925-0defea93325c/.

autonomous weapons are "incapable of abiding by the key principles of" *jus in bello*.[81] NGOs have actively and successfully promoted banning other weapons in recent years.[82]

Finally, much of the step-zero questioning arises in the writings of commentators, who may have distinct incentives. In particular, commentators often have incentives to make novel and interesting claims to spur discussion or generate debate. Moreover, commentators may be more willing to ask the step-zero question because they do not themselves face the need to operate weapons systems and conform their behavior to international law. Rethinking international law requirements from the ground up, as the step-zero question invites, may partly be a luxury that inheres to commentators and academics who stand apart from the operational issues they consider in their writings.

As these suggestions make clear, multiple differing parties, with very different interests, may each at various times and for various reasons have incentives to ask the step-zero question. With each new technology, *someone* will likely have an incentive to ask the step-zero question. The next Part turns from why the question is repeatedly asked to why the answer is generally the same.

C. The Persistence of the Answer

Despite the recurrent question about whether existing international law applies to new military technology, after the debate runs its course, the frequent answer seems to be to apply existing law.[83] Cyberwar seems poised to follow this pattern, though both the technological and legal issues continue to evolve.

As noted above, the official position of the United States is that existing *jus ad bellum* and *jus in bello* rules apply to cyber weapons.[84] The United States takes the position that cyber actions can constitute an armed attack and trigger a right to self-defense, and that IHL principles, such as proportionality and distinction, apply to cyber actions as they do to military actions undertaken with other weapons.[85] China, Russia, and other influential states in the U.N. GGE took a step toward this position by agreeing that the U.N. Charter, and therefore Articles 2(4) and 51, apply to cyber actions, though they have not agreed that existing *jus in bello* rules apply.[86] More recently, NATO has taken the position that existing rules of both *jus ad bellum* and *jus in bello* apply to cyberwarfare.[87]

Nongovernmental actors are also coalescing around the applicability of existing *jus ad bellum* and *jus in bello* rules. The NATO Cooperative Cyber Defence Center

---

81. *See* HUM. RTS. WATCH, *supra* note 34, at 30.

82. *See, e.g.*, Kenneth Anderson, *The Ottawa Convention Banning Landmines, the Role of International Non-Governmental Organizations and the Idea of International Civil Society*, 11 EUR. J. INT'L L. 91, 104–09 (2000) (chronicling NGOs' push for banning landmines in the Ottawa Convention).

83. *But see supra* notes 6–7 and accompanying text (discussing new law in the form of bans on particular types of weapons).

84. *See supra* text accompanying notes 49–52.

85. Koh, Remarks to USCYBERCOM Conference, *supra* note 52, at 3–5.

86. *See supra* note 58 and accompanying text.

87. *See supra* note 48.

of Excellence convened a group of international legal experts to develop the *Tallinn Manual on the International Law Applicable to Cyber Warfare* (*Tallinn Manual* or *Manual*).[88] The *Tallinn Manual* contains an extensive set of ninety-five blackletter rules that, in the consensus view of the legal experts who drafted the *Manual*, reflect customary international law.[89] The *Manual* takes the position that existing *jus ad bellum* and *jus in bello* rules apply to cyberspace.[90] It specifically notes that the experts unanimously agreed that "general principles of international law appl[y] to cyberspace" and rejected the position that "international law is silent on cyberspace in the sense that it is a new domain subject to international legal regulation only on the basis of new treaty law."[91]

Why, in the face of persistent consideration of the step-zero question, is the answer that existing law applies? Several main reasons may explain the persistence of the answer.

First, the *jus ad bellum* and *jus in bello* have proven adaptable in the past with the rise of new technologies and situations. As explained in Part I, a pattern of practice has developed to support application of existing law to new situations.[92] There is, in other words, a precedent for using precedent in the law of war context and perhaps therefore a path dependence to the outcome. In the nuclear weapons context, the ICJ explained that Articles 2(4) and 51 of the U.N. Charter "apply to any use of force, regardless of the weapons employed,"[93] and with respect to *jus in bello*, the Court specifically rejected the idea that the IHL provisions embodied in the Geneva Conventions do not apply because nuclear weapons were developed after the treaties were negotiated.[94] The Court recognized that "nuclear weapons were invented after most of the principles and rules of humanitarian law applicable in armed conflict had already come into existence," but explained that "it cannot be concluded from this that the established principles and rules of humanitarian law applicable in armed conflict did not apply to nuclear weapons."[95] The same logic justifies application of existing law to the military technologies, including cyber weapons, that States have developed since the advent of nuclear weapons.

Second, and relatedly, continuing to apply existing law is also attractive because of the persistence of the interests that the laws of war seek to protect. As the ICJ explained in considering nuclear weapons, to hold that IHL does not apply to nuclear

88. TALLINN MANUAL at 1.

89. *Id.* at 6.

90. *Id.* at 5.

91. *Id.* at 13.

92. *Cf.* STUART BANNER, WHO OWNS THE SKY?: THE STRUGGLE TO CONTROL AIRSPACE FROM THE WRIGHT BROTHERS ON 45 (2008) ("No legal issue is entirely new. Lawyers, accustomed to reasoning by analogy, can always find a precursor that is similar in some respects.").

93. Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226 para. 39 (July 8).

94. *Id.* para. 85.

95. *Id.* para. 86; *see also* Koh, Remarks to USCYBERCOM Conference, *supra* note 52, at 3 ("This is not the first time that technology has changed and that international law has been asked to deal with those changes. In particular, because the tools of conflict are constantly evolving, one relevant body of law—international humanitarian law, or the law of armed conflict—affirmatively anticipates technological innovation, and contemplates that its existing rules will apply to such innovation.").

weapons because they were developed after IHL rules "would be incompatible with the intrinsically humanitarian character of the legal principles in question which permeates the entire law of armed conflict and applies to all forms of warfare and to all kinds of weapons, those of the past, those of the present and those of the future."[96] Existing law was designed, for example, to protect civilians from the consequences of conflict. That concern transcends the type of weapon deployed. Thus, although the nature of the weapon has changed, the underlying concern has not, which reduces one possible justification for altering existing law.

Third, application of existing law is attractive because of the potential consequences of not doing so. In particular, because of the positivist, consent-based nature of international law,[97] it could be argued that in the absence of applicable law, a State's actions in cyberspace are unregulated until new law is developed.[98] This is a frightening prospect. States could take advantage of the period before new law is developed to act in ways utterly incompatible with IHL as it has developed over the past centuries. Starting from scratch to negotiate a new treaty for cyberspace could take years or even decades. The prospect of leaving States free to act without restraint during that period motivates arguments that such from-scratch development is unnecessary because existing law applies. Even if existing law is an imperfect means of regulating States' actions in cyberspace, imperfect law is preferable to no law at all.[99]

Fourth, and finally, while starting law development from scratch would be cumbersome and time consuming, application of existing law essentially provides a shortcut to a workable system of legal regulation of new war-fighting technology. Using existing law allows States to avoid the transaction costs of starting from scratch.[100] In many cases, application of existing law provides settled rules that can be applied to a new situation. Take, for example, the most basic rule regarding force: the prohibition on the threat or use of force contained in Article 2(4) of the U.N. Charter.[101] As States have recognized, the prohibition continues in force regardless of technological changes.[102] Agreement on the rule does not preclude disagreement about its application in particular circumstances, but it at least obviates the need to agree upon a new rule.

In other instances, applying existing law imports well-worn debates into a new context. For example, there is long-standing disagreement over the point at which a use of force constitutes an armed attack, and over whether there is a difference

96. Legality of the Threat or Use of Nuclear Weapons, 1996 I.C.J. 226 para. 86.

97. *See supra* Part II.B.1.

98. *See* SINGER, *supra* note 33, at 387 (suggesting that with respect to robots and the laws of war, "[t]he current 'legal limbo' . . . becomes a legal vacuum").

99. *See* Koh, Remarks at USCYBERCOM Conference, *supra* note 52, at 3 ("Cyberspace is not a 'law-free' zone where anyone can conduct hostile activities without rules or restraint.").

100. *See* Ashley Deeks, *The Geography of Cyber Conflict: Through a Glass Darkly*, 89 INT'L L. STUD. 1, 17 (2013) (explaining that the U.S. government often has "an inherent institutional instinct . . . to anchor novel legal situations in existing bodies of law and practice, and to reason by analogy. . . . Particularly where the analogies are quite reasonable (as they are between kinetic and cyber activities), it often is easier to draw from existing rules than to craft new ones from whole cloth.").

101. U.N. Charter art. 2, para. 4.

102. *See supra* note 58 and accompanying text.

between the two.[103] Applying existing law to the cyber context does not resolve this debate, but neither does it alter it in any meaningful sense. The commentary to the blackletter rules in the *Tallinn Manual*, which chronicles multiple instances in which old debates have been layered onto the new cyber context, notes disagreement among the experts group about, for example, the line distinguishing a use of force from an armed attack and particularly about whether the reported U.S. and Israeli Stuxnet operations against Iranian nuclear facilities constituted an armed attack or merely a use of force.[104] Even when the application of extant law imports existing debates, applying existing law is helpful because the debates themselves are well-settled: Each side understands the opposing position and where the points of disagreement arise.[105]

III. WHEN EXISTING LAW RUNS OUT: A CYBER–LAW OF WAR

As argued in Part I and documented in more detail with respect to cyberwar in Part II, the answer to the step-zero question in the law of war context is often the application of existing law. This is true with respect to the most fundamental principles of *jus ad bellum* and *jus in bello*, such as the right to self-defense and the principles of proportionality and distinction.[106] However, the characteristics of a new technology that make it qualitatively different from the war-fighting technology that has preceded it may also make it different in ways that require adjustment of more specific principles or adoption of entirely new rules particular to the new weapon. Application of existing law without modification is unlikely to be a complete answer to optimal regulation of a new weapon, such as a cyber weapon. But experience suggests that new law or modifications to existing law will constitute the minority of law applicable to the new technology.

For cyber operations, some new law or modifications to existing law may be needed to fill gaps or solve complications that cyber weapons create with respect to existing law. States and scholars are still in the early stages of figuring out when cyberwar-specific tweaks are needed and what exactly such tweaks should involve.[107] Some aspects of cyber weapons have no analogue in the non-cyber context. For

103. The International Court of Justice, for example, has distinguished between uses of force in general and armed attacks—"the most grave forms of the use of force." Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Merits, 1986 I.C.J. 14, para. 191 (June 27). The United States, on the other hand, has long taken the position that there is no difference between a use of force and an armed attack. *See, e.g.*, Abraham D. Sofaer, Legal Adviser, U.S. Dep't of State, The Sixth Annual Waldemar A. Solf Lecture in International Law: Terrorism, the Law, and the National Defense (May 4, 1989), *in* 126 MIL. L. REV. 89, 94 (1989) (criticizing the *Nicaragua* decision and explaining that the United States has "always construed the phrase 'armed attack' . . . consistent with a customary practice that enables any State effectively to protect itself and its citizens from every illegal use of force aimed at the State").

104. *See* TALLINN MANUAL r. 10 cmt. 9, r. 13 cmt. 13.

105. For additional examples from the *Tallinn Manual*, see Kristen E. Eichensehr, Book Review, 108 AM. J. INT'L L. 585, 586-87 (2014) (reviewing TALLINN MANUAL).

106. *See supra* Part II.C.

107. *See, e.g.*, Michael N. Schmitt, *The Law of Cyber Warfare:* Quo Vadis?, 25 STAN. L. & POL'Y REV. 269, 271 (2014) ("reflecting on key . . . norms that are most vulnerable to pressure for future interpretive adaptation" in the cyberwar context).

example, cyber weapons create the possibility of actions that cause severe harm to the victim, but nevertheless do not result in physical damage or injury to persons. The paradigmatic example is an attack that wipes out information stored on a system or network, such as a stock exchange. There is not yet agreement on whether to categorize such an incident as an armed attack.[108] It is possible that over time a cyber-specific definition of armed attack may arise that does not require physical harm, even though physical harm is required for armed attacks caused by other sorts of weapons.

Other aspects of existing law are rendered more complicated by the nature of cyberspace and may for that reason require modification. For example, the anonymity the Internet fosters makes attributing attacks to the real-world identity of attackers difficult (though not impossible),[109] and facilitates attackers' ability to route attacks through multiple—often innocent—servers around the world to make attacks appear as though they originated in countries other than their true origin.[110] Such manipulation of the source of an attack is impossible for other types of weapons, and the rules designed to deal with easily attributable attacks may need to be amended to address the new cyberwar challenges.

As these examples illustrate, there is likely to be a long process of working out how existing laws of war apply to cyberspace and to different factual scenarios in the cyber realm. This process may reveal instances in which existing laws of war are insufficient, though such insufficiencies will likely be the exception, rather than the rule.

As the process of working out how existing law applies to cyberspace proceeds, a cyber-law of war—that is, cyber-specific rules for armed conflict—might arise with respect to some legal rules. One potential cyber-specific alteration, as suggested above, would be to broaden the definitions of use of force and armed attack in the cyber context to encompass circumstances in which a cyber action causes no physical harm, but nonetheless causes severe damage of another kind.[111] The paradigmatic example of such an intrusion is a debilitating attack on a stock exchange or on major financial institutions. State practice may move toward considering such an incident to constitute a use of force or even an armed attack. If so, this would be a cyber-

108. *See* TALLINN MANUAL r. 12 cmt. 9 (noting that some of the experts took the position that physical damage is required to constitute an armed attack, while others "emphasized the catastrophic effects such a [stock exchange] crash would occasion and therefore regarded them as sufficient to characterize the cyber operation as an armed attack").

109. Discerning the source of even very sophisticated intrusions is possible with technical expertise and resources, as evidenced by recent reports that link specific units of China's People's Liberation Army to actions against U.S. companies, *e.g.*, MANDIANT, EXPOSING ONE OF CHINA'S CYBER ESPIONAGE UNITS 2 (2013), *available at* http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf; CROWDSTRIKE, CROWDSTRIKE INTELLIGENCE REPORT: PUTTER PANDA 4–5 (2014), *available at* http://resources.crowdstrike.com/ putterpanda/; *see also* Press Release, U.S. Dep't of Justice, U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage (May 19, 2014), *available at* http://www.justice.gov/opa/pr/2014/May/14-ag-528.html.

110. *See, e.g.*, Duncan B. Hollis, *An e-SOS for Cyberspace*, 52 HARV. INT'L L.J. 373, 397 (2011) ("Those with sufficient technical skill can remain anonymous at will. They can even leave behind a 'false flag,' implicating an otherwise innocent individual, group, or government.").

111. *See supra* note 108 and accompanying text.

specific rule because for conventional uses of force or armed attacks, physical damage would still be required.[112]

A second possibility for a cyber-law of war might be to amend the law on targeting of dual-use infrastructure. The United States has declared treatment of dual-use infrastructure in the cyber context an "unresolved question."[113] The *Tallinn Manual*, on the other hand, stakes out a definitive position: "An object used for both civilian and military purposes—including computers, computer networks, and cyber infrastructure—is a military objective."[114] It further explains, "This principle confirms that all dual-use objects and facilities are military objectives, without qualification."[115] The *Manual* takes care to explain that it sets out "the applicable *lex lata*, that is, the law currently governing cyber conflict," not "*lex ferenda*, best practice, or preferred policy,"[116] and the dual-use infrastructure targeting rule it sets out may be an instance in which the two diverge.

As the *Manual* explains, attacks against dual-use objects are subject to the requirement of proportionality and the requirement to take precautions in attacks.[117] However, it also gives the following example and analysis:

> Consider a network that is being used for both military and civilian purposes. It may be impossible to know over which part of the network military transmissions, as distinct from civilian ones, will pass. In such cases, the entire network (or at least those aspects in which transmission is reasonably likely) qualifies as a military objective. The analogy is a road network used by both military and civilian vehicles. Although an attacker may not know with certainty which roads will be travelled by enemy military forces (or which road will be taken if another is blocked), so long as it is reasonably likely that a road in the network may be used, the network is a military objective subject to attack. There is no reason to treat computer networks differently.[118]

Although there may be "no reason to treat computer networks differently" under existing law, there may be very good policy reasons to consider altering the rule to treat computer networks differently. As a practical matter, a military that uses bombs to target a particular road or road network is unlikely to discover the bombs intended for the target network hitting the intended target and then wandering onto other non-targeted road networks. The same is not true, however, of even very sophisticated code or other cyber actions. Call it the "wandering weapon" problem. For example, the Stuxnet attack against Iranian nuclear facilities was

112. For example, economic coercion in the form of sanctions would not be transformed into a use of force by the cyber-specific rule suggested above. *Cf.* CRAWFORD, *supra* note 65, at 747 (noting the "prevailing view" that the prohibition on the "threat or use of force" in the U.N. Charter "is confined solely to armed force" and "does not extend to political or economic coercion").

113. Koh, Remarks at USCYBERCOM Conference, *supra* note 52, at 8.

114. TALLINN MANUAL r. 39.

115. *Id.* r. 39 cmt. 1.

116. *Id.* at 5.

117. *See id.* r. 39 cmt. 2.

118. *Id.* r. 39 cmt. 3.

revealed when it infiltrated systems other than its targets due to coding errors.[119] On another occasion, a reported U.S. military operation to take down a site originally set up by the CIA and Saudi Arabia to monitor terrorist communications "inadvertently disrupted more than 300 servers in Saudi Arabia, Germany and Texas."[120]

More generally, the drafters of the *Tallinn Manual* recognized that the dual-use targeting rule they set out could "lead to the conclusion that the entire Internet can become a military objective if used for military purposes," though they viewed "the circumstances under which the Internet in its entirety would become subject to attack" as "so highly unlikely as to render the possibility purely theoretical at the present time."[121] Although proportionality and the precautionary principle should limit attacks on the Internet as a whole, even the *Tallinn Manual*'s drafters do not rule out the possibility that circumstances could justify an attack on the entire Internet at some point in the future.[122]

The importance of the Internet and certain other networks to civilian life may suggest that the normal rule that any dual-use object is a military target is unsatisfactory in the cyber context. The standards-based limitations of proportionality and the precautionary principle may allow too much discretion and create too much uncertainty as applied to the Internet as a whole or to particular kinds of networks. Technological uncertainty can make the conduct of proportionality calculations in the cyberspace context very difficult and unreliable. As an alternative to the usual standards-based limitations, a rule banning attacks on the entire Internet or particular kinds of networks—even if they are technically dual use—might be preferable to ensure that the balance is struck in favor of civilians in the heat of conflict.[123]

Moreover, in time, more experience with cyberwar may lead to determinations that particular types of cyber weapons cannot comply with the *jus in bello* and should therefore be banned. Bans on specific cyber weapons would follow a long-standing pattern in laws regulating the conduct of war. Beginning in the late nineteenth century, the international community regulated the conduct of hostilities not just with standards governing behavior, but also with treaty provisions prohibiting particular types of weapons determined to be incompatible with the principles of distinction, proportionality, or humanity. The Hague Conventions of 1899 prohibited poisoned arms,[124] dum-dum bullets,[125] and the use of projectiles that

119. *See* Sanger, *supra* note 46.

120. *See* Ellen Nakashima, *Dismantling of Saudi-CIA Web Site Illustrates Need for Clearer Cyberwar Policies*, WASH. POST, Mar. 19, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/03/18/A R2010031805464.html?sid=ST2010031901063.

121. TALLINN MANUAL r. 39 cmt. 5.

122. *Id.* (noting that "*virtually any* attack against the Internet would have to be limited to discrete segments thereof" (emphasis added)).

123. *Cf.* ROBERT K. KNAKE, COUNCIL ON FOREIGN RELATIONS, INTERNET GOVERNANCE IN AN AGE OF CYBER INSECURITY 23 (2010), *available at* http://www.cfr.org/terrorism-and-technology/internet-governance-age-cyber-insecurity/p22832 (suggesting possible future agreements to prohibit attacks on power grids, the financial sector, and root operations); SINGER & FRIEDMAN, *supra* note 38, at 191 (suggesting a limited agreement prohibiting attacks on banks because although "banks don't have an extra special immunity in the old laws of war the way hospitals do[,] . . . they may need to be treated as a special case in the virtual side of any new laws").

124. Hague Convention [No. II] with Respect to the Laws and Customs of War on Land art. 23, July

release "asphyxiating or deleterious gases."[126] More recent treaties have prohibited, for example, chemical weapons,[127] biological weapons,[128] "blinding laser weapons,"[129] anti-personnel landmines,[130] and cluster munitions.[131]

These existing weapons bans are unlikely to translate directly into the cyber context, except perhaps to the extent that a cyber attack could, for example, trigger the release of chemical weapons. But particular cyber weapons could pose the same compliance problems as other, now banned weapons. Existing bans stem from concerns about weapons that cause superfluous injury or are incapable of being used in a way that discriminates between military targets and civilians (e.g., a cloud of chemical weapons that disperses beyond military forces into civilian areas).[132] Similar concerns might apply to particular types of cyber weapons going forward, although the current information deficit about States' offensive cyber capabilities makes it difficult to identify specific types of cyber weapons that might produce the same concerns that motivated past weapons bans.

Cyberwar is not unique, however, in the inability to forecast which weapons will create concerns triggering a ban. The momentum for the existing treaties banning particular weapons typically built in the aftermath of conflict, after the weapons were used, produced horrible effects, and created a backlash. As one legal historian recently explained, "Laws of war typically come in the dismayed aftershock of conflict, not in the impassioned heat of battle.... Humanitarians usually fight the last war when they make rules for the next one."[133] Cyberwar is no different.

29, 1899, 32 Stat. 1803, 1 Bevans 247.

125. Hague Convention [No. IV], Declaration III on the Use of Bullets Which Expand or Flatten Easily in the Human Body, July 29, 1899, 26 Martens Nouveau Recueil (ser. 2) 1002, 187 Consol. T.S. 459, *available at* http://avalon.law.yale.edu/19th_century/dec99-03.asp.

126. Hague Convention [No. IV], Declaration II on the Use of Projectiles the Object of Which Is the Diffusion of Asphyxiating or Deleterious Gases, July 29, 1899, 26 Martens Nouveau Recueil (ser. 2) 998, 187 Consol. T.S. 453, *available at* http://avalon.law.yale.edu/subject_menus/lawwar19th_century/dec99-02.asp.

127. Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on Their Destruction, Jan. 13, 1993, S. TREATY DOC. NO. 103-21, 1974 U.N.T.S. 45.

128. Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on Their Destruction, *opened for signature* Apr. 10, 1972, 26 U.S.T. 583, 1015 U.N.T.S. 163.

129. Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects: Protocol on Blinding Laser Weapons art. 1, Oct. 13, 1995, T.I.A.S. No. 09-721.2, 2024 U.N.T.S. 167.

130. Convention on the Prohibition of the Use, Stockpiling, Production and Transfer of Anti-Personnel Mines and on Their Destruction, Sept. 18, 1997, 2056 U.N.T.S. 241.

131. Convention on Cluster Munitions, Dec. 3, 2008, 2688 U.N.T.S. 39.

132. *See* R.R. Baxter, *Conventional Weapons under Legal Prohibitions*, 1 INT'L SEC., Winter 1977, at 42, 47–48 (describing three criteria for banning particular weapons: 1) "whether the weapon causes unnecessary suffering or superfluous injury"; 2) "whether the weapon has indiscriminate effects"; and 3) "whether the weapon kills through treachery"); Detlev F. Vagts, *The Hague Conventions and Arms Control*, 94 AM. J. INT'L L. 31, 32 (2000) (noting that, at the time the Hague Conventions were negotiated, military officials were willing to prohibit "weapons that threatened to get out of control").

133. JOHN FABIAN WITT, LINCOLN'S CODE: THE LAWS OF WAR IN AMERICAN HISTORY 3 (2012).

CONCLUSION

As the technology of war-fighting inevitably progresses, history suggests that the step-zero question will arise with each new innovation. Military officials, States, NGOs, and commentators will raise the question of whether the new weapon is so qualitatively different from what has come before that the existing rules, designed for earlier technology, are incompatible with or incapable of satisfactorily regulating the use of the new weapon. As the examples set out in this Article illustrate, the answer to this question is likely to be no. The international community, after a period of debate and examination, will probably apply existing law with some tweaks around the edges, rejecting a fundamental re-writing of the existing laws of war, while reserving the possibility of banning entirely new weapons that cannot comply with existing legal rules.

In the end, applying existing law with minor revisions and extensions as necessary serves many values, including continuing to protect the fundamental interests that the laws of war seek to preserve, ensuring that weapons are regulated from the time of their first use, and providing a shortcut to a workable regulatory regime that, at worst, preserves existing disagreements.[134] Moreover, the process of considering and answering the step-zero question may have intrinsic value. As it has recurred even in the last decade, considering the step-zero question begins to look like a routinized process for decision-makers and commentators to hash out consensus on how international law will handle new technologies. The step-zero question is an action forcing event: It focuses attention, drives debate, and ultimately fosters the careful consideration that can lead to consensus about law moving forward. Many steps follow step zero, but we have to start somewhere.

134. *See supra* Part II.C.

"Use of Force" and "Armed Attack" Thresholds in Cyber Conflict: The Looming Definitional Gaps and the Growing Need for Formal U.N. Response

PRIYANKA R. DEV*

SUMMARY

* Priyanka R. Dev received the degree of Juris Doctor in 2015 at the University of Texas School of Law and is the Director of Development of the TEXAS INTERNATIONAL LAW JOURNAL.

INTRODUCTION

There is little disagreement that computer technology has dramatically altered the nature of international conflict. Today, governments can utilize social media to topple regimes,[1] use silent signals instead of people to commit espionage,[2] and wage wars with the simple click of a button.[3] And no State, corporation, or other organization—despite its resources or its military reputation—is immune from the threat of another. In early 2012, the websites of several big U.S. banking institutions fell prey to cyber intrusion when Iranian hackers launched a series of distributed denial of service (DDoS) attacks and captured computer clouds at data centers around the world, turning them into networks of slave computers, or botnets, positioned to flood and interrupt cyber traffic to and from the banking websites.[4] After the attacks, the Iranian group that took credit for them warned the world through online postings: "From now on, none of the U.S. banks will be safe from our attacks."[5] In light of incidents like this, U.S. defense officials view cyber attacks to be the "single greatest threat" to U.S. national security.[6]

As the dangers of cyber actions evolve in the wake of technological developments, so too should the way States and organizations apply traditional law of armed conflict (LOAC) principles to cyber actions. Traditional kinetic LOAC principles simply do not fit this new wave of warfare.[7] The limitations of applying traditional LOAC to cyber acts have left nation States misguided and confused, forcing them to rely on subjective views of what is lawful rather than apply an objective, internationally-accepted assessment of lawfulness before implementing a cyber act. In the absence of formal guidance from the United Nations, the organization that typically formalizes LOAC rules into transnational binding treaties,[8] scholars have offered informal rules of cyber conduct in the form of the

1. *See, e.g.*, Desmond Butler et al., *U.S. Secretly Created 'Cuban Twitter' to Stir Unrest*, ASSOCIATED PRESS (Apr. 4, 2014, 12:24 AM), http://bigstory.ap.org/article/us-secretly-created-cuban-twitter-stir-unrest (discussing a U.S.-engineered social media site designed for Cuban citizens to communicate and organize for renegotiating of the balance of power between the Cuban government and its citizens).

2. *See* James E. McGhee, *Cyber Redux: The Schmitt Analysis, Tallinn Manual and US Cyber Policy*, 2 J.L. & CYBER WARFARE 64, 64 (2013) ("[F]ocused cyber threats have resulted in exposed intellectual property, research and development, military plans, proprietary information and extortion.").

3. Bradley Raboin, *Corresponding Evolution: International Law and the Emergence of Cyber Warfare*, 31 J. NAT'L ASS'N ADMIN. L. JUDICIARY 602, 603 (2011) ("Now, with merely a computer and an Internet connection, an entire nation's infrastructure, both military and civilian, may be critically affected.").

4. Nicole Perlroth & Quentin Hardy, *Bank Hacking Was the Work of Iranians, Officials Say*, N.Y. TIMES, Jan. 8, 2013, http://www.nytimes.com/2013/01/09/technology/online-banking-attacks-were-work-of-iran-us-officials-say.html?pagewanted=1&_r=2.

5. QassamCyberFighters, *Phase/2,w/4; Operation Ababil*, PASTEBIN (Jan. 1 2013), pastebin.com/dwu47giH.

6. Jordain Carney, *Defense Leaders Say Cyber is Top Terror Threat*, NAT'L J. (Jan. 6, 2014), http://www.nationaljournal.com/defense/defense-leaders-say-cyber-is-top-terror-threat-20140106.

7. *See* Michael N. Schmitt, *Cyber Operations and the* Jus Ad Bellum *Revisited*, 56 VILL. L. REV. 569, 571 (2011) [hereinafter Schmitt, *Cyber Operations*] ("[T]he existing legal norms do not offer a clear and comprehensive framework within which states can shape policy responses to the threat of hostile cyber operations . . . . [I]nternational law as traditionally understood departs at times from what the international community would presumably demand in the cyber context.").

8. LTC DEAN L. WHITFORD ET AL., JUDGE ADVOCATE GENERAL'S LEGAL CTR. & SCH., U.S. ARMY, LAW OF ARMED CONFLICT DESKBOOK 29 (LTC William J. Johnson & LCDR David H. Lee eds., 2014).

Tallinn Manual[9]—but their response lacks the enforceability mechanisms that boost the legitimacy of and reciprocity for LOAC. While most States nonetheless urge support for the black letter rules in the *Tallinn Manual*, at least one—namely, Russia—rejects the *Tallinn Manual* based on its view that traditional LOAC is ill-fitted to deal with cyber conduct and awaits a more formal international response.[10] Whether or not one believes that traditional LOAC can be appropriately applied to the cyber warfare realm, most everyone agrees that an official U.N. Treaty approach—if it comes at all—could take years.[11]

Given this state of limbo, this paper synthesizes and assesses the various ways in which the traditional combat thresholds of a U.N. Article 2(4) "use of force" and an Article 51 "armed attack" have been applied to cyber conduct, ultimately highlighting the problems that arise from literally extending these established Charter principles to cyber acts. Part I introduces the existing sources of law around this issue but reveals the gaping hole that the United Nations has left with regard to cyber rules. Part II discusses, in detail, what amounts to an Article 2(4) use of force in the cyber context and, in light of the difficulties that arise from literally extending the term, suggests a new approach that better accounts for cyber damages. Part III discusses how scholars have defined an armed attack in the cyber context, pointing out the great problems of the existing ambiguity about when a state can legitimately respond in self-defense under Article 51. Part IV finally applies these working definitions as well as my proposed suggestions to a recent potentially unlawful cyber action. In exploring what types of actions currently do and, in the future, should trigger these important LOAC thresholds, this paper aims to bring some clarity to an area of cyber conflict law that even pioneering cyber conflict experts admit is filled with impractical, ill-defined principle thresholds.[12]

---

9. *See generally* TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE (Michael N. Schmitt ed., 2013) [hereinafter TALLINN MANUAL].

10. *See* Elena Chernenko, *Russia Warns Against NATO Document Legitimizing Cyberwars*, RUSS. BEYOND THE HEADLINES (May 29, 2013), http://rbth.com/international/2013/05/29/russia_warns_against_nato_document_legitimizing_cyberwars_26483.html (concluding that, based on statements by Russian Defense Ministry leaders, Russian authorities have taken a "guarded view" of the *Tallinn Manual* in part because they think its publication legitimizes the concept of cyberwars).

11. *See id.* (explaining that an agreement between the United States and Russia on cyberwar policy is unlikely to occur anytime soon); *cf.* Derek Jinks, Remarks at Texas International Law Journal Symposium Intangible Weaponry & Invisible Enemies: Applying International Law to Cyber Warfare, (Mar. 7, 2014), *available at* https://www.youtube.com/watch?v=bgM3EIYIRos (commenting that the secretiveness of States is one insurmountable problem preventing the international community from adopting a treaty resolving the rules governing cyberwarfare).

12. *See* Schmitt, *Cyber Operations*, *supra* note 7, at 571 ("Unfortunately, the existing legal norms do not offer a clear and comprehensive framework within which states can shape policy responses to the threat of hostile cyber operations."); TALLINN MANUAL intro. ("[T]he scope and manner of international law's applicability to cyber operations, whether in offence or defence, has remained unsettled since their advent.").

I. CURRENT SOURCES OF LAW AND AUTHORITY ON CYBER LAW OF ARMED CONFLICT

While the United Nation's response to cyber conflict and its dealing with the gaping hole in cyber LOAC has been nearly negligible,[13] there do exist several sources of authority, including the *Tallinn Manual*, individual nation state policy, and scholarly frameworks, which can help governments navigate their cyber conduct.

The authority that comes closest to an international response is the *Tallinn Manual on the International Law Applicable to Cyber Warfare*.[14] The *Tallinn Manual*, published in 2013 by a group of twenty renowned Western law scholars and practitioners (referred to as "The International Group of Experts"), contains ninety-five black letter rules about how States are to operate in a cyber warfare context;[15] the actual rules reflect the consensus on current customary international law as agreed upon by a majority of the scholars after consultation with treaty law, national military manuals, and studies by international humanitarian law agencies—to name a few of the sources.[16] The comment sections that follow each rule also contain minority viewpoints that were not integrated into the main rule.[17] Three organizations—the International Committee of the Red Cross (ICRC), the North Atlantic Treaty Organization (NATO), and United States Cyber Command—stood in as "observers" to the project,[18] which suggests that the project had a greater international voice than it actually did; but the rules do not necessarily reflect the positions of these internationally acclaimed organizations.[19] Moreover, while the *Tallinn Manual* seems generally well received,[20] the International Group of Experts did not include representatives from many of the countries that one might expect or wish to be included in a treatise on cyber warfare given their cyber capabilities, including Russia, China, and other eastern States.[21] And while the writers have already received criticism regarding this lack of diversity,[22] they did note that the

13. *See* TALLINN MANUAL intro. (explaining that "[t]here are no Treaty provisions that directly deal with 'cyber warfare'.").

14. *See* Jason Healey, *Reason Finally Gets a Voice: The Tallinn Manual on Cyber War, and International Law*, NEW ATLANTICIST (Mar. 27, 2013), http://www.atlanticcouncil.org/blogs/new-atlanticist/reason-finally-gets-a-voice-the-tallinn-manual-on-cyber-war-and-international-law ("The *Tallinn Manual*... —a novelty for the field of cyber statecraft—actually provides answers.").

15. *See generally* TALLINN MANUAL.

16. *Id.* intro.

17. *Id.*

18. *Id.*

19. *Id.*

20. Michael Schmitt, *The Law of Cyber Warfare:* Quo Vadis?, 25 STAN. L. & POL'Y REV. 269, 270 n.4 (2014); Healey, *supra* note 14.

21. The International Group of Experts did not include representatives from states located east of the former Iron Curtain. TALLINN MANUAL intro. Int'l Grp. of Experts (listing experts from institutions in the United States, the United Kingdom, Germany, Belgium, Canada, Australia, the Netherlands, Sweden, and Switzerland). The *Tallinn Manual* scholars respond to this criticism openly and honestly. They respond that the substantive differences regarding this interpretation of international law between the Western and Eastern worlds are not at all significant; because of this, the Eastern lack of representation on the committee does not affect the substance of the *Tallinn Manual*. Michael Schmitt, Remarks at Intangible Weaponry & Invisible Enemies: Applying International Law to Cyber Warfare, Texas International Law Journal Symposium (Mar. 6 2014), *available at* https://www.youtube.com/watch?v=M8qSLLPbuOQ [hereinafter Schmitt, Remarks at Texas International Law Journal Symposium].

22. Lauri Mälksoo, *The Tallinn Manual as an International Event*, DIPLOMAATIA (Aug. 2013),

Tallinn Manual was a work in progress and that, over time, state practice may alter the rules and norms articulated.[23] The writers even started a second edition not long after the first was published; unfortunately, it does not appear that any Eastern scholars are involved in the forthcoming set of revisions either.[24] The biggest limitation of the *Tallinn Manual*, despite its extremely comprehensive approach to defining a set of cyber LOAC, is that, as a scholarly project, it derives authority solely from academia rather than the sovereign authorities that have in the past served as a means of legitimating and enforcing LOAC principles.[25] The *Tallinn Manual*, therefore, despite its honorable contributions and its potential to lay the groundwork for a more formal U.N. Treaty, merely offers States persuasive secondary authority.[26]

Many States have unsurprisingly developed internal policies for cyber operations to help determine when another government's cyber actions have crossed a threshold of unlawfulness and, perhaps more importantly, when a lawful response to foreign state action is justified.[27] The United States, for instance, draws operational guidance from internal policy guidelines set by the executive branch.[28] Admittedly, analyzing individual state perspectives rather than a truly international response as to what types of cyber conduct constitute uses of force or armed attacks is inherently unhelpful in establishing an objective, worldwide threshold.[29] However,

---

http://www.diplomaatia.ee/en/article/the-tallinn-manual-as-an-international-event/ (reviewing the *Tallinn Manual*) ("The legal experts that wrote the Tallinn Manual have distinctly American and Old European backgrounds . . . . Some circles have already expressed criticism: Why did the project not involve legal experts for example from China or the Russian Federation?").

23. TALLINN MANUAL intro.

24. Schmitt, Remarks at Texas International Law Journal Symposium, *supra* note 21; *see also* Kristin Bergtora Sandvik, *New NATO Cyber Defense Policy: Unclear on Key Issues*, SWED. INST. INT'L AFF. (Oct. 14, 2014), http://www.ui.se/eng/blog/blog/2014/10/14/new-nato-cyber-defense-policy-unclear-on-key-issues.aspx (acknowledging criticism that the *Tallinn Manual* is the work of Western legal experts and discussing the high likelihood of the *Tallinn Manual's* revision effort—"Tallinn 2.0"—to produce another "invariably Western pronouncement[]").

25. The editors of the *Tallinn Manual* acknowledged this limitation. *See* TALLINN MANUAL intro. ("Ultimately, the [*Tallinn Manual*] must be understood as an expression solely of the opinions of the International Group of Experts, all acting in their private capacity.").

26. *Cf.* Brett Esptein, *The Rules of Cyber-Warfare: What are the Issues with These Rules, How Can the United States Respond to an Attack when Applying These Rules, and Should New Rules Be Enacted?*, 18 HOLY CROSS J.L. & PUB. POL'Y 247, 269–70 (2014) (stating that while the *Tallinn Manual* addresses "the lack of well-defined rules regulating cyber-warfare," it "is not binding on any nation").

27. *See, e.g.*, Convention on Cybercrime pmbl., Nov. 23, 2001, T.I.A.S. No. 13174, E.T.S No. 185 (discussing "the need to pursue, as a matter of priority, a common criminal policy aimed at the protection of society against cybercrime").

28. *See* Exec. Order No. 13636, 78 Fed. Reg. 11739 (Feb. 19, 2013) (tasking government agencies to construct a framework for reducing cyber-security risks to critical infrastructures); U.S. DEP'T OF ARMY, FIELD MANUAL 3-38: CYBER ELECTROMAGNETIC ACTIVITIES 3–10 tbl.3-3 (2014) [hereinafter FM 3-38] (detailing the involvement of the President and the Department of Defense in cyberspace operations); Harold Hongju Koh, Legal Adviser, U.S. Dep't of State, International Law in Cyberspace, Remarks at the USCYBERCOM Inter-Agency Legal Conference (Sept. 18, 2012), *available at* http://www.state.gov/s/l/releases/remarks/197924.htm (discussing the U.S. Department of State's understanding that *jus ad bellum* rules apply to cyberspace).

29. *Cf.* McGhee, *supra* note 2, at 64 (stating that a "hodgepodge of cyber concepts, definitions, rules, policy and law" is not compatible with the development of an international law of cyber warfare).

these internal policies still serve as important sources of law for individual state policy and may help guide any future U.N. or international response.

Even scholarly work by cyber experts, though it lacks any mechanism for enforcement, is important to consider as a source of guiding law around cyber actions;[30] it could also serve States and ultimately the United Nations with innovative solutions for assessing cyber acts. In a field that is constantly evolving, scholarly work on cyber conduct can provide a platform of ideas, conceptualizations, and innovative guidance for States to draw from before integrating certain standards into policy. While much of the scholarship on cyber uses of force and armed attacks was properly incorporated into and thereby supplanted by the *Tallinn Manual*,[31] it is nonetheless important to note that there are still new ideas emerging from scholarly work that should be integrated into whatever final approach is ultimately taken by the United Nations or another binding authority.

II. BACKGROUND PRINCIPLES FROM KINETIC LAW OF ARMED CONFLICT THRESHOLDS

First, it is essential to discern what the terms "use of force" and "armed attack" traditionally entail and, perhaps most importantly, to distinguish between the two.[32] The use of force threshold draws meaning from Article 2(4) of the U.N. Charter, which states the following: "All Members shall refrain in their international relations from the threat or *use of force* against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations."[33] Article 2(4) therefore recognizes that the principle of national sovereignty underscores all our LOAC rules;[34] out of this language, it has become generally accepted that it is when a State's conduct rises to the threshold of a use of force that LOAC is triggered.[35] Traditionally, an unlawful use of force justifies some countermeasures, such as economic sanctions or U.N. intervention, but it does not

30. *See generally, e.g.*, Schmitt, *Cyber Operations*, *supra* note 7.

31. For example, Michael N. Schmitt's seven-factor approach to determining whether an act was an Article 2(4) use of force, originally articulated in an article for The Columbia Journal of Transnational Law, was integrated into the *Tallinn Manual* at Comment 9 to Rule 11. TALLINN MANUAL r. 11 cmt. 9 (citing Michael N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 COLUM. J. TRANSNAT'L L. 885, 914 (1999)).

32. Some contend that the concepts of "use of force" and "armed attack" are essentially indistinguishable. *See* TALLINN MANUAL r. 11 cmt. 7 (acknowledging the view contrary to the *Tallinn Manual*'s rules that "the distinction between the two concepts is either so narrow as to be insignificant or non-existent," and as a result, "any illegal use of force can qualify as an armed attack"). But, for purposes here, the two concepts will be referred to separately and refer to two different thresholds of activity, as is in line with current customary international law. *Id.*

33. U.N. Charter art. 2, para. 4 (emphasis added).

34. *See* M.P. Ferreira-Snyman, *The Evolution of State Sovereignty: A Historical Overview*, 12 FUNDAMINA 1, 24 (2006) ("[T]he ban on the use of force by the Charter is today understood not so much as a limitation of sovereignty, but as a necessary prerequisite for a *de facto* enjoyment of sovereign equality by states. Therefore, a state's sovereign equality depends on a comprehensive prohibition of the use of force and an effective mechanism to implement and enforce this prohibition.").

35. *See* Michael N. Schmitt, *"Attack" as a Term of Art in International Law: The Cyber Operations Context*, *in* 4TH INTERNATIONAL CONFERENCE ON CYBER CONFLICT 283, 286 (C. Czosseck et al. eds., 2012) [hereinafter Schmitt, *"Attack" as a Term of Art*] ("[A]n 'armed attack' is an action that gives States the right to a response rising to the level of a 'use of force,' as that term is understood in the *jus ad bellum*.").

justify a typical counterattack, even if it is in proportion to the initial use of force.[36] It is also generally accepted that not all types of pressure, including political or economic, are sufficient to amount to unlawful Article 2(4) uses of force.[37]

The perpetration of an armed attack provides States with a different legal threshold[38] and draws its significance from U.N. Charter Article 51. Article 51 provides the following: "Nothing in the . . . Charter shall impair the inherent right of individual or collective self-defence if an *armed attack* occurs against a Member of the United Nations . . . ."[39] Under this provision, then, a state can lawfully and proportionately respond to an act that meets the threshold of unlawfulness of an armed attack.[40] Under traditional LOAC, therefore, when State A commits an armed attack against State B, State B can lawfully respond *proportionately* to State A's act.[41] Because an armed attack invokes a right to respond in a manner that could cause more harm in addition to that of the initial attack, it is generally accepted that an armed attack entails a higher threshold of unlawfulness than that of an Article 2(4) use of force, to which a state is not granted the right to lawfully respond through similar proportionate means.[42] An armed attack also typically requires some sort of physical damage to persons or property in order to qualify as such.[43]

There is general agreement that the U.N. Charter, even though it was conceived around kinetic principles, also applies to cyber conduct.[44] Customary law, guided by the *Nuclear Weapons Advisory Opinion* issued by the International Court of Justice (ICJ), demonstrates that Article 2(4) applies to "any use of force, regardless of the weapons employed."[45] It is likewise difficult to find scholarship that suggests that Article 51 armed attacks are not relevant in the cyber context.[46] So, while it is fairly evident that the international community agrees that these concepts apply to and therefore place limits on a State's right to act against another State through cyber means, there is still much ambiguity in the discussions about *how* these concepts apply.

---

36. TALLINN MANUAL r. 9.

37. *Id.* r. 11 cmt. 2.

38. Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, para. 210 (June 27) (noting that there are "measures which do not constitute an armed attack but may nevertheless involve a use of force").

39. U.N. Charter art. 51 (emphasis added).

40. *See* Schmitt, *"Attack" as a Term of Art*, *supra* note 35, at 286 (stating that defensive force may be used in response to an armed attack when non-forceful means are likely to prove inefficient and when such defensive force is proportional to the attack incurred).

41. *Id.*

42. *Id.* at 285.

43. TALLINN MANUAL r. 13 cmt. 9.

44. *See, e.g.*, MARCO ROSCINI, CYBER OPERATIONS AND THE USE OF FORCE IN INTERNATIONAL LAW 115 (2014) (stating that cyber attacks are "prohibited by Article 2(4) of the UN Charter").

45. Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226, para. 39 (July 8).

46. *Cf.* Schmitt, *Cyber Operations*, *supra* note 7, at 571, 589 (noting that the May 2010 U.S. National Security strategy considers cyber threats the most serious national challenge and arguing that cyber operations with sufficient consequence are armed attacks).

III. THEORIES ON WHAT CONSTITUTES A CYBER "USE OF FORCE"

The gamut of theories about how States should determine if a particular act qualifies as a use of force, though diverse, does not yet account for the crucial need to expand the analysis from a physical results-based approach to a more encompassing one that takes into account non-physical damage. Given that relatively few cyber acts result in the type of physical harm or damage that States traditionally accept as unlawful,[47] States will ultimately be forced to adopt one of two solutions in order to proportionately apply the use of force threshold to cyber attacks: (A) expand the definition of an Article 2(4) use of force to account for the types of damages, like financial ones, that cannot be physically discerned and traditionally do not make an act more likely to be a use of force; or (B) create a *new* legal threshold below use of force that justifies a state response to a cyber act that is an invasion on national sovereignty but does not meet the threshold of a traditional Article 2(4) violation. I discuss these solutions in turn below.

A. Expanding the Existing Article 2(4) Definition of "Use of Force"

In order to best account for the full scope of potential damages but still recognize only the traditional Article 2(4) thresholds, States would have to broaden the accepted definition of an Article 2(4) use of force. Looking solely at an act's physical effects to determinate if a cyber act qualifies as a use of force might be common sense, but this approach does not properly respond to the reality that there are non-physical effects of cyber attacks that are equally harmful to State sovereignty. What I coin the "common-sense approach" was best summarized by former U.S. State Department Legal Advisor Harold Koh, who suggested that if the *effects* of an action under kinetic law would constitute use of force, then the cyber equivalent is also a use of force.[48] Koh's explanation, however, does not seem to provide for the possibility that there are acts whose effects under kinetic law would not result in a use of force, but their cyber equivalents would meet the threshold.[49] Koh's explanation only makes clear that a cyber act which results in injury or death to persons or damage or destruction to objects is, by established definitions, an Article 2(4) use of force.[50]

Customary international law seems to be in consensus with the common-sense approach but similarly is unclear as to whether physical damage is required.[51] The *Tallinn Manual* suggests that the writers saw this issue as a source of deep

47. Russell Buchan, *Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?*, 17 J. CONFLICT & SECURITY L. 211, 211–13 (2012).

48. *See* Koh, *supra* note 28 (stating that *jus ad bellum* rules to apply to uses of force in cyberspace and noting instances where the physical effects of cyber acts are comparable to physical kinetic acts).

49. Koh explained the common-sense approach with this simple example: If a line of malicious code from a distant computer somehow broke a dam and flooded a civilian population, it would constitute a use of force because the kinetic equivalent of a bomb exploding and leading to similar damage would also reach the threshold. *Id.*

50. *Id.*

51. *See* TALLINN MANUAL r. 11 (explaining that the scale and effects approach is used to determine whether there was a use of force).

contention.[52] The comments to the *Tallinn Manual* indicate that its writers believed certain cyber acts that would not ordinarily result in the type of purely physical damage required under kinetic law should nonetheless constitute uses of force, in part because of the special nature of potential destruction through computers.[53] Yet, as the writers often realized, *lex lata*, or the law as it stood at the time of their drafting the rules, did not allow for them to incorporate this understanding of use of force into the black letter law; instead, they were locked in to traditional definitions.[54] Other scholars have commended the *Tallinn Manual* editors for synthesizing customary international law on this topic but also criticized—and I think properly so—the editors' very limited definition of an Article 2(4) use of force.[55]

Ignoring non-physical damages in analyzing whether an act is an Article 2(4) use of force would be a great disservice to the unfortunate realities of cyber warfare; if the international community chooses to simply extend existing use of force definitions to cyber activity, it must adopt a broader conception of what damages to analyze. This common-sense approach does not consider the detrimental extent of non-physical damage that can result from cyber acts.[56] For instance, under the common-sense approach, a cyber infiltration of State A by State B that resulted in total paralysis of State A's stock market but no direct physical damage would not constitute a use of force; yet, a bomb attack in one tiny town in State A would not only qualify as a use of force, but perhaps also rise to the level of an Article 51 armed attack.[57] The *Tallinn Manual* definition similarly legitimizes a strange policy: If State A, through some sort of cyber act, prevented fuel from being delivered to an airplane, which was necessary for State B to carry out a planned, pre-determined kinetic attack, the cyber act would still not constitute a use of force. Under

52. Even the *Tallinn Manual* editors could not agree on a definitive view. *See id.* intro. ("[T]he lack of agreed-upon definitions, criteria, and thresholds for application[] creates uncertainty when applying the *jus ad bellum* to the rapidly changing realities of cyber operations.").

53. *See id.* r. 10–11 & cmts. (elaborating on the ways that cyber operations are similar and different from traditional uses of force).

54. *See id.* intro. (noting that the experts were bound to write the rules in line with *lex lata* rather than preferred policy, or *lex ferenda*). *Tallinn Manual* Rule 10 provides the following: "A cyber operation that constitutes a threat or use of force against the territorial integrity or political independence of any State, or that is in any other manner inconsistent with the purposes of the United Nations, is unlawful." *Id.* r. 10. Rule 11 then goes on to define use of force, but this definition is reminiscent of the overly simplified analog that the U.S. State Department provided: "A cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force." *Id.* r. 11; *cf.* Koh, *supra* note 28 (suggesting that a cyber action constitutes a use of force if the effects of an equivalent kinetic action would constitute a use of force).

55. *See, e.g.*, McGhee, *supra* note 2, at 84 ("[The *Tallinn Manual*] spells out, with great particularity, its application and non-application to certain areas of law and conflict. Of note, the Group limits their discussion to use of force and armed conflict . . . . This ignores the overlap and fusion of electronic warfare and cyber warfare capabilities, an issue of great interest within the military Services.").

56. For instance, cyber campaigns can disrupt services to a State by targeting key infrastructure, causing devastating economic effects. *See, e.g.*, JAMES A. LEWIS, CTR. FOR STRATEGIC & INT'L STUDIES, THRESHOLDS FOR CYBERWAR 2 (Sept. 2010), *available at* http://csis.org/files/publication/101001_ieee_insert.pdf.

57. *See* Jay P. Kesan & Carol M. Hayes, *Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace*, 25 HARV. J.L. & TECH. 415, 516–17 (2012) (discussing that whether or not a cyber attack rises to the threshold of a use of force may depend upon whether one analyzes the attack in terms of its economic effects or by measuring whether the damage caused could have been created by a kinetic attack).

traditional LOAC definitions, the purely economic consequences of a cyber event escape consideration even though they could be as harmful to a nation state and result in proximate harm to the citizens' persons and property.[58]

There are several other policy reasons why the threshold for a cyber use of force cannot be taken directly from kinetic LOAC as the *Tallinn Manual* suggests.[59] First, cyber rules in general should expand to include consideration of more attenuated damage or harm when qualifying an act as a use of force.[60] The physical damage or harm requirement is only appropriate in a kinetic context, where it is easier to discern when there are kinetic weapons involved.[61] In the cyber context, where attribution itself presents a complication,[62] the physical harm or damage presents a more attenuated, proximate cause rather than a direct cause.[63] Moreover, while civilian populations are not necessarily affected by kinetic acts because they enjoy the protections of the traditional LOAC principle of distinction,[64] cyber acts often affect civilian populations without harming them under traditional LOAC.[65] These effects, because they are often secondary or tertiary consequences without a physical element, do not make an act any more unlawful, though they should.[66] Further, traditional thresholds must also shift because of the nature of the weapon being used.[67] While kinetic acts produce fairly instantaneous damage, using computers as weapons often results in more drawn-out, long-term effects;[68] traditional LOAC allows States no way to incorporate these long-term effects into their analysis of lawfulness.[69] A State's lawfulness assessment is therefore dictated by how quickly a weapon can produce an effect rather than by how deeply the effects penetrate and cause more harm over time.[70]

The comments to the *Tallinn Manual* present a respectable solution to expanding the scope of the current definition of an Article 2(4) use of force. Though

---

58. *See* TALLINN MANUAL r. 11 cmt. 10 (discussing that highly invasive operations causing mere inconvenience are not categorized as a use of force, but "some may categorize massive cyber operations that cripple an economy as a use of force, even though economic coercion is presumptively lawful")

59. TALLINN MANUAL r. 11.

60. See McGhee, *supra* note 2, at 72–73 (explaining that limiting use of force analysis to physical effects produces illogical results because both the physical effects of kinetic attacks and the economic effects of cyber attacks can create the same negative consequences for a population).

61. *See id.* at 72–73 (explaining that cyber operations can have the same overall effects as kinetic strikes "without causing lasting physical damage or damage at all").

62. *Id.* at 78–79.

63. *Id.* at 74–75.

64. The principle of distinction, which "requires states to distinguish civilian and military personnel and restrict attacks to military objectives," presents a challenge in the cyber warfare context. Oona A. Hathaway et al., *The Law of Cyber-Attack*, 100 CAL. L. REV. 817, 851–52 (2012).

65. *See* McGhee, *supra* note 2, at 72–73 ("Thus, two events that cause the exact same consequences would, in fact, be treated differently under [LOAC] rules . . . .").

66. *Id.* at 74–75; *see also* Jody R. Westby, *We Need New Rules of Engagement for Cyberwar*, N.Y. TIMES (Mar. 1, 2013,), http://www.nytimes.com/roomfordebate/2013/02/28/what-is-an-act-of-cyberwar/we-need-new-rules-of-engagment-for-cyberwar (advocating for international law reform because cyber warfare does not fit neatly within the LOAC framework).

67. *See generally* Westby, *supra* note 66.

68. McGhee, *supra* note 2, at 73–75.

69. *See id.* at 88–91 (discussing the difficulties of evaluating lawfulness for States with regard to cyber attacks).

70. *See id.* at 73–74 ("Can semi-autonomous delayed effect cyber capabilities register on the immediacy criterion continuum for meeting use of force or armed attack?").

in no way binding or said to constitute black letter law, the comments actually imagine a broader conceptualization of use of force,[71] which seems more useful in the cyber context. First, the scholars suggest a focus on the scale and effects of an act.[72] Comment 2 to Rule 11 notes that "mere economic or political coercion" should be insufficient.[73] Comment 9 also enumerates a very broad set of factors, including the severity and quantifiable nature of the consequences of the act, which a state could and should consider when determining whether its cyber action may constitute a use of force.[74] I list and summarize the factors below:

1. Severity	Analyze the level of harm or damage that was caused to individuals and property, with an eye towards the scale, scope, and duration of *consequences*.
2. Immediacy	Analyze whether the act had more immediate effects or consequences; if a violated state was given the opportunity to avoid or forestall the consequences (i.e., the consequences were less immediate), it is less likely that the act should constitute a use of force.
3. Directness	Analyze how direct the causation between the initial act and resulting consequences is; the more direct, the more likely it should constitute a use of force
4. Invasiveness	Analyze the degree to which a network system was penetrated; the penetration of a classified system should fall closer to a use of force than that of a declassified system.
5. Measurability	The more quantifiable and identifiable the consequences, the more likely the act is to constitute a use of force.
6. Presumptive Legitimacy	Consider whether the act is presumptively unlawful; if the act is explicitly unlawful, then the act is more likely to constitute a use of force.
7. State Responsibility	The greater the state involvement in the act, the greater the threat to international stability and the more likely the act is to constitute a use of force.[75]

This model, though it contains a more expanded definition of use of force, might work fine in after-the-fact analysis, but because of the amount of detail required to perform a thorough analysis through the factors, it is not very helpful for operational, game-time decision making.

An alternative way to integrate the economic realities of computer network interruptions in setting the thresholds of cyber activity might be to adopt a dollar-

71. TALLINN MANUAL r. 11 & cmts.
72. *Id.* cmt. 1.
73. *Id.* cmt. 2.
74. *Id.* cmt. 9.
75. *Id.*

based approach to damages.[76] For instance, if instead of weighing factors, States quantified damages and losses to help determine whether an act constituted a use of force both before and after a cyber act, they would be forced to integrate the financial consequences of cyber activities into their operational decisions.

A 2013 incident in which the Syrian Electronic Army hacked into The Associated Press's Twitter account, causing a huge hit to U.S. stock markets, may best highlight the usefulness of this dollar-based approach.[77] On April 23, 2013, the Syrian Electronic Army allegedly hacked The Associated Press's Twitter account to post untrue tweets telling the world that there had been an attack on the White House.[78] In response to the false news, the Dow Jones plunged by 150 points, and the single "fake tweet erased $136 billion in equity market value."[79] Though the effects of the act were temporary (the stock market response was later described as a "perilous but short-lived nosedive"),[80] the situation does suggest that the case of true economic harm should perhaps rise to the level of use of force; but the only way to incorporate financial harm into the use of force threshold is to accept it in lieu of physical damage.

Under a dollar-based approach, if the total value of loss to network connectivity and the immediate financial repercussions exceed the dollar amount threshold, the act would constitute a use of force; but if the dollar amount of damage falls below the threshold, there is no presumption of an Article 2(4) violation. I only propose this alternative to the physical damage requirements imposed under *lex lata* in order to suggest that the realities of economic harm, given the growing interdependence of world economies,[81] have become increasingly severe. The corresponding response to this gaping hole in the rules of cyber conduct should integrate economic harm into the equation. But integrating economic harm by re-defining use of force still asks us to stretch traditional concepts[82] that may not stretch that far.

B. Creating a New Threshold Below "Use of Force"

An alternative solution to better encapsulate non-physical cyber effects, rather than expanding ill-fitted traditional concepts, would be for the international

---

76. *See* Thomas Dübendorfer et al., *An Economic Damage Model for Large-Scale Internet Attacks*, *in* PROCEEDINGS OF THE THIRTEENTH IEEE INTERNATIONAL WORKSHOP ON ENABLING TECHNOLOGIES: INFRASTRUCTURE FOR COLLABORATIVE ENTERPRISES 223, 225 (2004) (discussing an economic damage model that proposes to measure damages caused by large-scale Internet attacks, such as Distributive Denial of Service (DdoS) attacks, by attempting to enumerate downtime loss, disaster recovery, liability, and customer loss).

77. Max Fisher, *Syrian Hackers Claim AP Attack that Tipped Stock Market by $136 Billion: Is It Terrorism?*, WASH. POST, Apr. 23, 2013, http://www.washingtonpost.com/blogs/worldviews/wp/2013/04/23/syrian-hackers-claim-ap-hack-that-tipped-stock-market-by-136-billion-is-it-terrorism/. It should be noted that the Syrian Electronic Army never formally claimed responsibility for the act, but there is informal evidence that the group was the perpetrator. *Id.*

78. *Id.*

79. *Id.* (quoting OptionsBeat, Bloomberg News, TWITTER (Apr. 23, 2013, 12:23 PM), https://twitter.com/OptionsBeat/status/326778407461474304).

80. *Fisher*, supra note 77.

81. *Globalization and Interdependence*, U.N. DEP'T ECON. & SOC. AFF., http://www.un.org/en/development/desa/oesc/globalization.shtml (last visited April 25, 2015).

82. *See* TALLINN MANUAL r. 11 cmt. 10 ("[E]conomic coercion is presumptively lawful.").

community to create a new threshold for actions that do not meet the traditional use of force threshold but nonetheless constitute a "breach of the peace" under Article 39 of the U.N. Charter.[83]

This solution, however, still requires that we stretch existing language from the U.N. Charter. Article 39 of the Charter enables the Security Council to authorize countermeasures in response to a situation that constitutes a "threat to the peace, *breach of the peace*, or act of aggression."[84] Under customary law, an Article 39 violation does not necessarily reach the requisite unlawfulness of an Article 2(4) use of force violation, but the question of what actions constitute a breach of the peace even in a kinetic context is still widely contested.[85] What constitutes a mere *threat* to the peace, though most agree it should be distinguished from an Article 2(4) use of force, is perhaps even more ill-defined.[86] The only formal guidance on what constitutes a breach of the peace appears in *Prosecutor v. Tadic*, an opinion of the International Criminal Tribunal for the Former Yugoslavia, but this guidance was too broad.[87] The court there stated that a threat to the peace should be assessed according to the "Purposes and Principles of the Charter";[88] however, the purposes listed in Article 1 cover a broad base of policies from solving social problems to developing friendlier world relations.[89] Allowing these breach of the peace violations to provide recourse to States affected by cyber acts would enable States to respond somehow when cyber operations harm individuals or property but not in a physical way.[90] There may still be disagreement as to whether intrusions of sovereignty that do not actually harm the target nation—those that are more akin to espionage—amount to an Article 39 violation,[91] but at least acknowledging the possibility of a cyber breach of the peace would allow States recourse to mitigating action.[92]

Perhaps the seemingly broad language of Article 39 and the wide discretion given to the Security Council in *Tadic* provide a better starting point from which to extend traditional U.N. Treaty principles to fit cyber acts. Adopting this solution

83. U.N. Charter art. 39 (authorizing the Security Council to determine the existence of a "breach of the peace" and to make recommendations to restore international peace and security).

84. *Id.* (emphasis added). The Article actually allows the Security Council to make recommendations or decide what measures are to be taken based on a list of forceful and non-forceful options in Articles 41 and 42 in order to restore national peace and security. *Id.*

85. *See* Schmitt, *Cyber Operations*, *supra* note 7, at 583 (discussing the difficulty of characterizing non-physical harm as an Article 39 threat to the peace).

86. *Id.*

87. *See* Prosecutor v. Tadić, Case No. IT-94-1-I, Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, para. 29 (Int'l Crim. Trib. for the Former Yugoslavia Oct. 2, 1995) (stating that the Security Council has wide but not unlimited discretion in characterizing an instance as a breach of the peace).

88. *Id.*

89. U.N. Charter art. 1, paras. 2–3; *see also* Schmitt, *Cyber Operations*, *supra* note 7, at 583–84 (describing the Purposes and Principles of the U.N. Charter as including "such intangibles as developing friendly relations and solving social problems").

90. *See* Schmitt, *Cyber Operations*, *supra* note 7, at 584 (describing how the Security Council "may label any cyber operation a threat to the peace" even though a cyber attack is not a physical attack).

91. *See id.* (stating that "[t]here are no territorial limits on situations which may constitute threats to the peace" and that "a threat to the peace is whatever the [Security] Council deems it to be").

92. *See id.* (explaining that the Security Council could authorize interruption of cyber communications as a measure that would maintain or restore peace and security in the event of a cyber threat or attack).

would allow States to avoid the well-defined, results-based approaches to harm under traditional Article 2(4) use of force analyses;[93] there would be no need to broaden "harm" past the scope of its customary kinetic interpretation. Instead, States could have alternate recourse by charging certain cyber acts that breach sovereignty as unlawful breaches of peace and seek U.N. recourse or the authority to lawfully respond via minor countermeasures.[94]

The 2012 Iranian attacks against U.S. banking institutions, and the subsequent U.S. response, demonstrate the need for and the usefulness of creating this third category.[95] In response to the attacks, the Obama administration was precautious and, instead of launching counter-botnets against Iranian computers that could trigger even worse counter-attacks, the United States convinced more than 100 other countries to "choke off" the intrusive computer traffic that stemmed from computer network nodes located in their respective countries.[96] It was largely a defensive, rather than an offensive, move that was made out of fear towards the "unintended consequences" of cyber activity;[97] officials later claimed they were wary of an "overly aggressive response that could invite escalatory attacks that might further paralyze the networks of American businesses."[98] But the response successfully hindered the Iranian attack, and because of this, officials refer to it as a "template" to respond in other similar cyber cases.[99]

I urge here that this template is an all-too-cautious one, and if the United States had access to a more legitimate, treaty-based justification for a stronger response, perhaps based on a third category of cyber activity under Article 39, it would have been able to respond more proportionately. The highly defensive strategy it adopted, in the absence of more formal thresholds, will do little to prevent the possibility of future, similar attacks on the United States;[100] without proper recourse against cyber acts, States are left vulnerable to repeated attacks. In the cyber realm just as much as in the kinetic one, a country's ability to take proper countermeasures allows the country to demonstrate military power and deter further action. Even in the cyber world, the ability to outwardly exercise national sovereignty and instill fear through military power should not be thwarted just because these actions lack a physical element or face ill-defined thresholds.

---

93. Article 2(4) extends only to "those threats of a use of force that would otherwise be unlawful," which would exclude cyber attacks and threats. *Id.* at 572.

94. McGhee, *supra* note 2, at 89 ("It would make little or no sense to allow states to use cyber in response to use of force and armed attacks, but to limit the tools available for lesser offenses."); *see also* Michael Gervais, *Cyber Attacks and the Laws of War*, 1 J.L. & CYBER WARFARE 8, 60–62 (2012) (suggesting that, although States' responses to low-intensity cyber attacks are constrained, they can and will respond to less severe attacks as they accumulate).

95. *See* Ellen Nakashima, *U.S. Rallied Multinational Response to 2012 Cyberattack on American Banks*, WASH. POST, Apr. 11, 2014, http://www.washingtonpost.com/world/national-security/us-rallied-multi-nation-response-to-2012-cyberattack-on-american-banks/2014/04/11/7c1fbb12-b45c-11e3-8cb6-284052554d74_story.html (reporting that the United States' response to Iranian botnet attacks on U.S. financial institution websites was measured and precautious).

96. *Id.*

97. *Id.*

98. *Id.*

99. *Id.*

100. *See id.* (reporting that former U.S. defense officials critiqued the U.S. response to the 2012 Iranian cyber attacks as weak).

Of course, acknowledging a cyber breach of the peace under Article 39 would not subject *every* cyber act to scrutiny as being unlawful. Just as traditional espionage, for instance, is not considered an unlawful breach of the peace or national sovereignty,[101] cyber LOAC should not expand so far as to treat cyber espionage that does not result in any disruption in networking[102] as unlawful by itself. For an example of cyber conduct that is intrusive but not a breach of sovereignty, one can look to recent conduct by the United States Agency for International Development (USAID). News reports indicate that in April 2013, USAID launched and backed a Cuban Twitter-like social media website to encourage dissent against the sovereign Cuban government.[103] Under the theories here, this act, without any quantifiable or physical harm, would not constitute either an Article 2(4) use of force or an unlawful act under the theoretical third threshold of Article 39. Defining common international standards for unlawful versus lawful activity in a cyber context will also help States ensure that their ongoing cyber espionage activities do not rise to or exceed the lawfulness threshold.

IV. THEORIES ON WHAT CONSTITUTES A CYBER "ARMED ATTACK"

Under customary international law, an armed attack as referenced in Article 51 constitutes a higher threshold of unlawfulness and only an armed attack, not an Article 2(4) use of force, legitimizes use of force in self-defense.[104] Any use of force in self-defense is of course still subject to conventional notions of military necessity and proportionality.[105]

Customary law appropriately incorporates both scale and effects into its conception of an Article 51 armed attack.[106] Rule 13 of the *Tallinn Manual* states, "A

101. *See* Schmitt, *Cyber Operations*, *supra* note 7, at 576 ("Although highly invasive, espionage does not constitute a use of force (or armed attack) under international law absent a nonconsensual physical penetration of the target state's territory, as in the case of a warship or military aircraft which collects intelligence from within its territorial sea or airspace. Thus, actions such as disabling cyber security mechanisms to monitor keystrokes would, despite their invasiveness, be unlikely to be seen as a use of force.").

102. McGhee, *supra* note 2, at 89 ("[W]hen *aren't* cyber operations subject to LOAC? The most obvious and relevant answer is, when the operation is conducted as espionage."); *see also*, *e.g.*, Gervais, *supra* note 94, at 89–90 (acknowledging that nations may engage in some *ruse du guerre* cyber tactics that do not violate LOAC).

103. Butler, *supra* note 1.

104. The International Court of Justice (ICJ) takes the position that there is a substantive distinction between a use of force and an armed attack and that not all uses of force warrant unilateral self-defense. Gervais, *supra* note 94, at 36 (citing Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, para. 206 (June 27)). But even under kinetic law, there is some disagreement about what exactly triggers a State's right to self-defense. *See*, *e.g.*, *id.* at 35–36 (noting that some scholars argue that any use of force is *per se* an armed attack); Michael N. Schmitt, *International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed,* 54 HARV. INT'L L.J. ONLINE 13, 21–22 (2012) [hereinafter Schmitt, *International Law in Cyberspace*] (discussing the disagreement between the U.S. government, which believes that any use of force constitutes an armed attack justifying self-defense, and the International Group of Experts, which agrees with the ICJ that there are separate thresholds for uses of force and armed attacks).

105. *Gervais*, *supra* note 94, at 57; *see also supra* Part II.

106. Schmitt, *International Law in Cyberspace*, *supra* note 104, at 18–22.

State that is the target of a cyber operation that rises to the level of an armed attack may exercise its inherent right of self-defence. Whether a cyber operation constitutes an armed attack depends on its scale and effects."[107] This majority rule mandates that, when a State is to evaluate whether or not another State's act was an armed attack, it is customary to take into account not only the *effects* of an action but also the *scale* of the action.[108] The *Tallinn Manual* comments suggest that an armed attack requires a trans-border element[109] and does not necessarily involve weapons.[110] Rule 30 actually defines an armed attack as that which is reasonably expected to cause "injury or death to persons or damage or destruction to objects."[111] Comment 9 to Rule 13 admittedly states that "[t]he case of actions that do not result in injury, death, damage, or destruction, but which otherwise have extensive negative effects" is an "unsettled" classification.[112]

However, it is noteworthy that existing cyber definitions of armed attack at least adopt a more comprehensive approach and incorporate not only direct but also proximate effects in the analysis. Comment 10 to Rule 13 states that the majority of the International Group of Experts concluded that "all reasonably foreseeable consequences of the cyber operation" are to be considered when one is analyzing whether an act meets the threshold; this suggests a broader proximate view than direct causation.[113] The Group, however, seemed divided as to whether an armed attack had to be *intentional*; the majority concluded that intention was irrelevant while the minority found intention to be required.[114]

James McGhee, an operational cyber law attorney for the U.S. Air Force, cautions against an overly-narrow approach to defining cyber attacks, suggesting that an odd outcome would result if one were to require direct physical damage for a cyber action to constitute an attack: A cyber event that blows out a power grid without any physical damage would not constitute a cyber attack, but a kinetic event that does the same thing would.[115] Yet, even though the *Tallinn Manual* suggests a slightly broader approach, the law is in flux.[116] As McGhee noted, these divisions within the law make it "possible to arrive at separate and contradictory answers of whether an event constitutes an attack."[117] And, as a result of the multi-faceted ambiguity and the numerous questions left unanswered, there have been no cyber acts that have been unanimously considered armed attacks by the international community.[118]

---

107. TALLINN MANUAL r. 13.

108. *Id.* cmt. 6.

109. *Id.* cmt. 2.

110. *Id.* cmt. 4.

111. *Id.* r. 30.

112. *Id.* r. 13 cmt. 9.

113. TALLINN MANUAL r. 10 cmt. 13.

114. *Id.* cmt. 11.

115. McGhee, *supra* note 2, at 73.

116. *See* William Banks, *The Role of Counterterrorism Law in Shaping* Ad Bellum *Norms for Cyber Warfare*, 89 INT'L L. STUD. 157, 162 (2013) (stating that, with regard to cyber warfare, "the legal regime remains clouded and ambiguous").

117. McGhee, *supra* note 2, at 100.

118. TALLINN MANUAL r. 13 cmt. 13.

The most recent wave of U.S. military policy adopted a surprisingly broad approach to the definition of cyber attack[119]—one that proves useful in discerning a definition that incorporates all facets of "effects."[120] In Joint Publication 3-12, the U.S. Department of Defense (DoD) defined a cyberspace attack as "[c]yberspace actions that create various direct denial effects in cyberspace (i.e., degradation, disruption, or destruction) and manipulation that leads to denial that is hidden or that manifests in the physical domains."[121] This definition provides a good platform for States because it accounts for the special nature of computer networking[122] and takes into account the devastating effects that harm other than physical harm can involve.[123] However, the DOD's definition might be problematic because it alone does not seem to delineate between various thresholds—for instance, what attacks constitute mere Article 2(4) uses of force versus Article 51 armed attacks. And, of course, because this definition originates with unilateral U.S. policy, it is unclear whether this definition is portable across the international community. Nonetheless, it provides a nice example of a step towards a more pragmatic solution in the current "hodge-podge of cyber concepts, definitions, rules, policy and law" that prevents proper development of international cyber warfare law.[124]

V. THE NEED FOR MORE DEFINED LAWFULNESS THRESHOLDS: LESSONS FROM STUXNET

The various thresholds of unlawful cyber activity were tested most famously in the 2010 Stuxnet malware virus incident.[125] There is some consensus in the international community that the 2010 Stuxnet operation was an armed attack, in part because, though the trigger occurred in cyber space, the virus ended up causing physical damage to targets.[126] In June 2010, the world discovered that the Stuxnet

119. *See* McGhee, *supra* note 2, at 94–97 (stating that "almost anything in cyber could constitute an attack" under the definition of "cyber attack" according to the military's Joint Publication 3-12); *see generally* JOINT CHIEFS OF STAFF, JOINT PUBLICATION 3-12 (R): CYBERSPACE OPERATIONS [hereinafter JP 3-12].

120. *See* McGhee, *supra* note 2, at 97 ("[T]he definition [of cyber attack] does not tell one whether those listed effects are the only effects allowed or whether more exist.").

121. JP 3-12, *supra* note 119, at II–5.

122. *See* McGhee, *supra* note 2, at 100 (explaining that the definition of attack dictated by U.S. policy includes events which do not manifest physically—for instance, those that cause a change in data "to reflect something different to the observer than what is actually there").

123. *See id.* at 72–73 (noting that a cyber event, such as the remote take down of a power grid, can lead to non-physical, yet devastating effects).

124. *Id.* at 102.

125. *See* Holger Stark, *Mossad's Miracle Weapon: Stuxnet Virus Opens New Era of Cyber War*, SPIEGEL ONLINE (Aug. 8, 2011), http://www.spiegel.de/international/world/mossad-s-miracle-weapon-stuxnet-virus-opens-new-era-of-cyber-war-a-778912.html (discussing the Stuxnet virus, the "first digital weapon of geopolitical importance" and its potential impact on future warfare).

126. Andrew C. Foltz, *Stuxnet, Schmitt Analysis, and the Cyber "Use-of-Force" Debate*, JOINT FORCE 4TH QUARTER 2012, 44; *see also* Kim Zetter, *Legal Experts: Stuxnet Attack on Iran Was Illegal 'Act of Force'*, WIRED (Mar. 25, 2012), http://www.wired.com/2013/03/stuxnet-act-of-force/ (reporting that the North Atlantic Treaty Organization (NATO) defense center designated the Stuxnet cyber attack an "act of force" that "likely violate[d] international law, according to the Tallinn Manual on the International Law Applicable to Cyber Warfare"). *But see* Shaun Waterman, *U.S.-Israeli Cyberattack on Iran Was 'Act of Force,' NATO Study Found*, WASH. TIMES, Mar. 24, 2013, http://www.washingtontimes.com

virus, a wireless malware virus that was able to transcend public Internet, attacked programmed computers at Iran's largest nuclear facilities and caused large-scale breakdowns in Iran's nuclear operations.[127] The malware worm, described as a "sophisticated computer program designed to penetrate and establish control over remote systems in a quasi-autonomous fashion," targeted computer programming systems at Iran's nuclear facilities—ultimately entirely reprogramming many of the systems struck.[128] The bug invaded the computers, lurked for days or weeks, and ultimately sent instructions to speed the nuclear centrifuges up or slow them down so that they started spinning at supersonic speeds and ultimately self-destructed.[129] One German expert that studied Stuxnet described it as a "military-grade cyber missile that was used to launch an 'all-out cyber strike against the Iranian nuclear program.'"[130] With the click of a button, a conglomerate of State and non-State actors, allegedly including the United States and Israel, managed to bring major breakdown to Iran's Natanz nuclear fuel enrichment plant, with some estimates indicating that the Stuxnet worm led to a 23% decline in the number of operating centrifuges between mid-2009 and mid-2010.[131]

The common-sense approach to the Article 2(4) use of force analysis, as well as customary law as reflected in the *Tallinn Manual*, suggests that the incident was an Article 2(4) use of force.[132] Because of the resulting physical damage, which would help constitute a use of force in a kinetic context, the direct application of this threshold to the Stuxnet incident points in the same direction. Even the factors laid out in the comments to the *Tallinn Manual* support a similar conclusion:

1.	Severity	Strong. Severe harm to property; weak harm to persons, but this factor allows for harm to property to constitute sufficiently strong consequence.
2.	Immediacy	Strong. Stuxnet damaged the computers it struck immediately, without allowing the computer user or facility managers to prepare or mitigate the consequences.
3.	Directness	Strong with regards to first-level damage. Much weaker with regard to secondary and tertiary systemic damage. Because the virus spread so easily [at times by itself], secondary and tertiary damages were exponential, but their importance is muted by this factor.

/news/2013/mar/24/us-israeli-cyberattack-on-iran-was-act-of-force-na/?page=all (reporting that Michael Schmitt, *Tallinn Manual* lead editor, told the Washington Times that the writers of the *Tallinn Manual* were unanimous that Stuxnet was an act of force, "[b]ut they were divided on whether its effects were severe enough to constitute an 'armed attack'").

127. *See* James P. Farwell & Rafal Rohozinski, *Stuxnet and the Future of Cyber War*, 53 SURVIVAL: GLOBAL POL. & STRATEGY 23, 29 (2011) (examining Stuxnet's effect on Iranian nuclear facilities, citing reports of temporarily-ceased uranium feeding, and speculating that a "decline in the number of operating [Iranian] centrifuges" for a period may be attributable to the virus attack).

128. *Id.* at 24.

129. Foltz, *supra* note 126, at 44.

130. Farwell & Rohozinski, *supra* note 127, at 23.

131. *Id.* at 29.

132. TALLINN MANUAL r. 11 cmt. 8

4.	Invasiveness	Strong suggests use of force. Stuxnet struck and completely controlled computer-programming systems.
5.	Measurability	Medium. While the consequences are identifiable [network failure was traceable to Stuxnet], they were not quantifiable.
6.	Presumptive Legitimacy	Weak/not applicable. No presumptive legitimacy or illegitimacy.
7.	State Responsibility	Weak. Unclear the degree of state involvement.[133]

However, while the *Tallinn Manual* rules and a strict application of traditional LOAC to Stuxnet suggest that the incident was an Article 2(4) use of force, the international community is still left utterly confused as to whether it rose to the threshold of armed attack.[134] The *Tallinn Manual* charges us with looking at both the scale and effects of the act,[135] but the Stuxnet incident reveals that some questions are still unresolved: From what chronological point of a large-scale attack does one assess whether the threshold of armed attack has been satisfied? Even among the proximate effects, what extent of effects does one take into account? Is it legitimate to treat the subversive nature of the attack as evidence of an armed attack rather than a less severe breach of the peace or use of force?

Some might even argue that Stuxnet was simply a pre-emptive cyber strike in self-defense in response to the threat of Iran's nuclear program;[136] yet, it does not seem that Iran's activities were at all imminent, which would be required to constitute a lawful act of self-defense under Article 51.[137] Even so, the lawfulness of Stuxnet as a preemptive cyber strike ultimately turns on whether the consequences of the act were proportional to the perceived threat[138]—a determination drawn from traditional LOAC that back then and even now remains foggy at best.[139]

While Stuxnet demonstrated the international community's need for better tools to preemptively assess the lawfulness of States' cyber actions and reactions, more recent news about the United States' reaction to Iran's intrusion on its financial

133. *Id.* r. 11 cmt. 9.

134. *See* Farwell & Rohozinski, *supra* note 127, at 32–33 (questioning whether action as a recourse to a cyber attack is allowed under Article 2(4) of the U.N. Charter).

135. TALLINN MANUAL r. 11.

136. *Id.* r. 13 cmt. 13 ("In light of the damage they caused to the Iranian centrifuges, some members of the International Group of Experts were of the view that the operations had reached the armed attack threshold (*unless justifiable on the basis of anticipatory self-defence . . .*)" (emphasis added)).

137. *Id.* r. 15.

138. A State may only resort to proportionate countermeasures to a perceived threat. *Id.* r. 9.

139. "The principle of proportionality stems from Article 51 of Additional Protocol I, which states that force is prohibited where it 'may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated.'" Gervais, *supra* note 94, at 84–85 (quoting Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I) art. 51(5), June 8, 1977, 1125 U.N.T.S. 3). Some courts take the view that there is a "zone of proportionality" within which a State has discretion to act. Gervais, *supra* note 94, at 85–86 (citing HCJ 2056/04 Beit Sourik Vill. Council v. Gov't of Isr. 58(5) PD 807 [2004] (Isr.)).

institutions in 2012[140] only further underscores the fact that States are left misguided. The Obama administration's response may have been altogether different if the United States had treaty protocols and more delineated principles to follow. If these cyber treaty protocols—hopefully elaborated sometime in our distant future—integrate consideration of the wide variety of intrusions on sovereignty that can occur as a result of cyber activity, States will be in a much better place to assess their own actions as well as those of intruders.

CONCLUSION

The latest cyber rumblings around the conflict in Crimea underscore that almost every modern conflict will involve some sort of cyber activity.[141] A week after Russia supposedly entered the Crimea region, Ukrainian security alleged that unknown cyber attackers were interfering with the mobile phone services of Ukrainian Parliament members.[142] In April 2014, reports indicate that Russian forces used hacking to intercept a U.S. surveillance drone that was over the Crimea region.[143] Not only has warfare evolved, but it also continues to evolve, and these new types of cyber activities make international recognition of cyber lawfulness thresholds even more critical to a legitimate LOAC tradition.

Given this influx, "[s]tates contemplating cyber operations, or that are the target thereof, must be highly sensitive to the international community's probable assessment of whether the operations violate the prohibition on the use of force."[144] In order to properly assess the international community's reaction, a State must be able to reasonably determine if its plan meets the threshold of a breach of the peace or rises to the level of an Article 2(4) use of force, and, if the plan entails force, whether it is a proper use of force in self-defense to an armed attack under Article 51. The reciprocity and therefore the legitimacy of LOAC rests upon more delineated and accepted notions of lawful thresholds within the realm of cyber activities.

Even outside of preserving the LOAC tradition, it is incumbent upon organizations like the United Nations to meet the evolving nature of military operations, especially as States are increasingly contributing resources into developing cyber operations.[145] In April 2014, the U.S. Army launched the Cyber Center for Excellence at Fort Gordon, the location where it plans to house all military doctrine writers for electronic warfare, signals, and cyber operations.[146] The Army also recently published field manual FM 3-38, *Cyber Electromagnetic Activities*, a response to the increasingly wireless nature of cyber operations and an

140. Perlroth & Hardy, *supra* note 4.

141. *See generally* Isaac R. Porche III, *Cyberwarfare Goes Wireless*, U.S. NEWS & WORLD REPORT (Apr. 4, 2014), www.usnews.com/opinion/blogs/world-report/2014/04/04/russia-hacks-a-us-drone-in-crimea-as-cyberwarfare-has-gone-wireless (describing cyberwarfare developments, including the increase in wireless cyberspace acts, and the U.S.'s operational military responses to these developments).

142. Peter Bergen & Tim Maurer, *Cyberwar Hits Ukraine*, CNN (Mar. 7, 2014), http://www.cnn.com/2014/03/07/opinion/bergen-ukraine-cyber-attacks/.

143. Porche, *supra* note 141.

144. TALLINN MANUAL r. 11 cmt. 8.

145. *See, e.g.*, Porche, *supra* note 141, (describing cyberwarfare developments, including the increase in wireless cyberspace acts, and the United States' operational military responses to these developments).

146. *Id.*

acknowledgement of the "broad and rapidly changing operational environment" that requires the Army to "leverage an electromagnetic spectrum that is increasingly competitive, congested, and contested."[147] The manual organizes infrastructure around cyber operations, setting up tactical cells that are to be filled with special personnel trained in electronic warfare.[148] Moves like this indicate that military operations all over the world are increasingly and rightfully responding to the impact that technological developments have on modern warfare. But, despite international scholars' and independent States' best efforts at responding to the developments, it unfortunately may be years before other well-recognized international authorities with greater enforcement mechanisms like the United Nations attempt to fill the void through formal treaty powers. Until then, the customary protocols around the various activity thresholds should shift to meet the realities of our changing conflict landscapes.

147. FM 3-38, *supra* note 28, at v.

148. *See generally id.*

Doing Business with a Bad Actor: How to Draw the Line Between Legitimate Commercial Activities and Those that Trigger Corporate Complicity Liability

SABINE MICHALOWSKI*

* Professor of Law, University of Essex. I would like to thank my colleagues Geoff Gilbert, Karen Hulme, and Sheldon Leader for their critical and very helpful comments on previous drafts of this Article.

ABSTRACT

One of the most complex and highly debated problems in the context of corporate liability for complicity in human rights violations is how to distinguish lawful commercial activities from those that give rise to corporate complicity liability. In many cases in which corporations are accused of aiding and abetting human rights violations, the act of assistance consists of what would usually be regarded as an ordinary and perfectly acceptable business activity, such as providing financing to a government or supplying it with goods or infrastructure. Merely doing business with a bad actor is not sufficient to impose liability on corporations for that actor's human rights violations, but no clear criteria on what transforms legitimate business transactions into reprehensible acts of complicity exist.

This Article approaches the question of determining the relevant liability standards by providing an in-depth analysis of jurisprudence stemming from three different contexts: Alien Tort Statute (ATS) cases on corporate complicity; ad hoc international criminal tribunals on the closely related question of dual-purpose act liability (where the assistance provided could be used for both lawful and unlawful activities); and U.S. criminal cases where the act of assistance consisted of a commercial activity. Jurisprudence stemming from these three different contexts has in common that many courts feel that the generally applicable standards for determining complicity liability need to be adapted and restricted where assistance consists of a commercially motivated or a dual-purpose act. This is largely achieved by requiring either that the assistance reach a certain significance threshold (limitations at the actus reus level of liability), or that the mental state with which it was carried out made the assistance particularly reprehensible (limitations at the mens rea level of liability).

In the particular context of corporate complicity liability in human rights violations, academic debate of liability standards largely focuses on whether the relevant mens rea standard should be one of purpose or one of knowledge. While clearly important, this Article goes beyond this question and argues that the mens rea standard cannot be understood and determined in isolation. Without taking a holistic look at all elements of liability and their interaction, it is not possible to sufficiently understand the concerns that triggered adoption of a purpose standard of mens rea, the legitimacy of these concerns, and alternative ways of addressing them.

The purpose of this Article is not to present detailed liability criteria that will work equally in all contexts. Rather, it serves the more modest aim of analyzing and drawing conclusions from the implications of different approaches to determining the necessary actus reus and mens rea elements of corporate complicity liability,

while recognizing that the details need to be developed with reference to the specific contexts in which the question of corporate complicity liability arises.

INTRODUCTION

Corporate complicity in human rights violations has received a lot of attention in recent years.[1] Complicity means that the corporation does not itself commit human rights violations, but rather assists others in carrying them out.[2] It thus relates to the situation of indirect corporate involvement in human rights abuses and frequently arises in the context of business transactions with "bad actors," often states, which commit gross human rights violations.[3] Assistance can take many different forms and can range from acts that only marginally impact the act carried out by the principal to those without which the principal offense would not be possible.

One of the most complex and highly debated problems in this context is how to distinguish lawful commercial activities from those that give rise to corporate complicity liability. In many cases in which corporations are accused of aiding and abetting human rights violations, the act of assistance consists of what would usually be regarded as an ordinary and perfectly acceptable business activity, such as providing financing to a government or supplying it with goods or infrastructure.[4] This raises the question of what transforms legitimate business transactions with governments (or in some instances other actors, such as armed groups) into reprehensible acts of complicity.

It is instantly obvious that the problem is not mainly legal in nature. Rather, how the law responds depends decisively on highly political and ideologically-fraught questions, such as whether and to what extent it is legitimate to pursue business interests, even if this has an adverse human rights impact. There might also be perfectly legitimate reasons for supplying governments, even those with the worst human rights records, with certain goods and services, such as to enable them to carry out governmental tasks that clearly benefit the population, like building schools. Are corporations, and should they be, responsible for how their business partners use their goods and services? If so, under what circumstances, and on what grounds?

More clarity on how to distinguish complicity from legitimate business transactions is of the utmost importance for various reasons. Corporations need to

---

1. *See generally* Special Representative of the Secretary-General on the Issue of Human Rights and Transnational Corporations and Other Business Enterprises, *Clarifying the Concepts of "Sphere of Influence" and "Complicity"*, Hum. Rts. Council, U.N. Doc. A/HRC/8/16 (May 15, 2008) (by John Ruggie) [hereinafter Ruggie, *Clarifying the Concepts*]; Special Representative of the Secretary-General on the Issue of Human Rights and Transnational Corporations and Other Business Enterprises, *Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework*, principle 17 & cmt., Hum. Rts. Council, U.N. Doc. A/HRC/17/31 (Mar. 21, 2011) (by John Ruggie) [hereinafter Ruggie, *Guiding Principles*]; 3 INT'L COMM'N OF JURISTS, CORPORATE COMPLICITY & LEGAL ACCOUNTABILITY (2008).

2. Ruggie, *Clarifying the Concepts*, *supra* note 1, para. 29–30.

3. *See* 3 INT'L COMM'N OF JURISTS, *supra* note 1, at 28 (noting that allegations of complicity might arise when companies transact business with bad actors who commit human rights violations).

4. *Id.* at 28–29.

be given clear guidance on their responsibilities, not just to avoid criminal and civil complicity claims, but also to be in compliance with human rights standards in highly significant soft law instruments, such as the U.N. Guiding Principles on Business and Human Rights, which include a responsibility to avoid complicity in human rights violations.[5] Courts need to have a good understanding of the policy implications of the choice and application of liability standards in this context, which is more and more important given that civil or criminal litigation against corporations is increasingly initiated in different states.[6] States need to know where their responsibilities lie when regulating corporate behavior and providing remedies for potential corporate abuse. And victims need to know under what circumstances they might have claims for damages against corporations that were complicit in the human rights violations they suffered.

At the judicial level, this problem has to date most explicitly, extensively, and influentially been addressed under the U.S. Alien Tort Claims Act (Alien Tort Statute, or ATS)[7] which for many years has been the most significant vehicle worldwide to address corporate complicity through litigation.[8] Despite the uncertain future of corporate complicity litigation under the ATS since the U.S. Supreme Court decision in *Kiobel*,[9] an analysis of cases decided in this context remains

5. Ruggie, *Guiding Principles*, *supra* note 1, principle 17 & cmt. For a critical discussion see generally Sabine Michalowski, *Due Diligence and Complicity: A Relationship in Need of Clarification*, *in* HUMAN RIGHTS OBLIGATIONS OF BUSINESS: BEYOND THE CORPORATE RESPONSIBILITY TO RESPECT? 218 (Surya Deva & David Bilchitz eds., 2013) [hereinafter Michalowski, *Due Diligence*].

6. For Canada *see*, *e.g.*, Anvil Mining, Ltd. v. Association canadienne contre l'impunité, 2012 QCCA 117 (Can. Que. C.A.) (deciding case concerning human rights abuses in the Democratic Republic of the Congo). For the United Kingdom, *see*, *e.g.*, Guerrero v. Monterrico Metals PLC, [2010] EWHC (QB) 3228 (deciding suit regarding conduct in Peru); *see also* Charis Kamphuis, *Foreign Investment and the Privatization of Coercion: A Case Study of the Forza Security Company in Peru*, 37 BROOK. J. INT'L L. 529, 542–48 (2012) (discussing the *Guerrero* case). For the Netherlands, *see*, *e.g.*, Hof 's-Gravenhage 9 mei 2007, NJFS 2007, 183 m.nt (van Anraat) (Neth.) (deciding case concerning conduct of Dutch citizen in Iraq); *see also* Wim Huisman & Elies van Sliedregt, *Rogue Traders: Dutch Businessmen, International Crimes and Corporate Complicity*, 8 J. INT'L CRIM. JUST. 803, 807–10 (2010) (discussing cases involving conduct abroad tried by Dutch courts).

7. The Alien Tort Statute (ATS), which provides that "[t]he district courts shall have original jurisdiction of any civil action by an alien for a tort only, committed in violation of the law of nations or a treaty of the United States," has been one of the main legal tools used to try to hold corporations to account for their complicity in violations of the law of nations. 28 U.S.C. § 1350 (2012); *see generally*, *e.g.*, Presbyterian Church of Sudan v. Talisman Energy, Inc., 582 F.3d 244 (2d Cir. 2009) (applying the ATS in an action against a Canadian corporation for complicity liability); Khulumani v. Barclay Nat'l Bank, Ltd., 504 F.3d 254 (2d Cir. 2007) (overturning the district court's dismissal of the claim under the Alien Tort Claims Act); Doe I v. Unocal Corp., 395 F.3d 932 (9th Cir. 2002) (finding a violation under the Alien Tort Claims Act).

8. 3 INT'L COMM'N OF JURISTS, *supra* note 1, at 54; *see* Alan O. Sykes, *Corporate Liability for Extraterritorial Torts under the Alien Tort Statute and Beyond: An Economic Analysis*, 100 GEO. L.J. 2161, 2162 (2012) ("Recent years have witnessed an enormous increase in litigation against corporate defendants under the Alien Tort Statute.").

9. Kiobel v. Royal Dutch Petroleum Co., 133 S. Ct. 1659, 1665 (2013) (holding that the presumption against the extraterritorial application of U.S. legislation applies to the ATS.) This has serious repercussions because in many of the cases filed under the ATS all relevant acts of assistance were committed abroad. Many courts have rejected ATS-based claims against corporations after *Kiobel* because of these extra-territoriality concerns. *See generally* Mujica v. AirScan Inc., 771 F.3d 580 (9th Cir. 2014); Baloco v. Drummond, 767 F.3d 1229 (11th Cir. 2014); Cardona v. Chiquita Brands Int'l, Inc., 760 F.3d 1185 (11th Cir. 2014); Chowdhury v. Worldtel Bangl. Holding, Ltd., 746 F.3d 42 (2d Cir. 2014); Balintulo v. Daimler AG, 727 F.3d 174 (2d Cir. 2013); Adhikari v. Daoud & Partners, No. 09–cv–1237,

important, and not only because corporate complicity cases continue to be brought under the ATS. More importantly, these cases constitute the most detailed engagement of a judiciary with the question of how to distinguish lawfully doing business with a bad actor from commercial activities that trigger complicity liability for human rights violations committed by a business partner.[10] Furthermore, this jurisprudence has highly influenced global attempts to conceptualize corporate liability.[11] The importance of understanding the relevant policy considerations identified by these courts, and their implications for defining legal principles and standards in this context, thus transcend ATS litigation and U.S. courtrooms. Part I of this Article will therefore provide a detailed analysis of selected ATS cases and assess different approaches to liability standards based on the policy considerations these approaches reflect.

While only ATS cases have expressly dealt with the question of corporate complicity in human rights violations, courts in other contexts had to deal with comparable issues. The ad hoc international criminal tribunals, for example, on whose analysis of liability standards for aiding and abetting liability ATS jurisprudence heavily relies, have recently struggled to apply these principles to so-called dual-purpose assistance cases, i.e., cases in which the accomplice provided "general assistance which could be used for both lawful and unlawful activities."[12] These have many similarities with the typical scenario in corporate complicity cases. Where, for example, military vehicles are sold to a regime that, to the seller's knowledge, uses such vehicles both for lawful and unlawful purposes, it is not clear what link between the sale and the unlawful use would be necessary to justify complicity liability of the seller. Part II of this Article demonstrates that the approaches developed by the ad hoc tribunals to resolve this question, based largely on policy considerations on how to establish a sufficient link between the act of assistance and the violation carried out by the principal, provide an interesting basis for reflection on liability standards for corporate complicity in human rights violations. The same is true for U.S. domestic criminal complicity cases where the act of assistance consists of a commercial act, and some of these cases and the policy discussions that informed the courts' approaches to defining liability standards in this context will therefore be discussed in Part III.

2013 WL 4511354 (S.D. Tex. Aug. 23, 2013); Kaplan v. Cent. Bank of the Islamic Republic of Iran, 961 F. Supp. 2d 185 (D.D.C. 2013); Hua Chen v. Honghui Shi, No. 09 Civ. 8920(RJS), 2013 WL 3963735 (S.D.N.Y. Aug. 1, 2013). Others courts have found that the facts sufficiently touched and concerned the U.S. to rebut the presumption against extra-territoriality. *See generally* Mastafa v. Chevron Corp., 770 F.3d 170 (2d Cir. 2014); Al Shimari v. CACI Premier Tech., Inc., 758 F.3d 516 (4th Cir. 2014); Krishanti v. Rajaratnam, No. 2:09–cv–05395, 2014 WL 1669873 (D. N.J. Apr. 28, 2014); Du Daobin v. Cisco Sys., Inc., 2 F. Supp. 3d 717 (D. Md. 2014); Ahmed v. Magan, No. 2:10–cv–00342, 2013 WL 4479077 (S.D. Ohio Aug. 20, 2013); Sexual Minorities Uganda v. Lively, 960 F. Supp. 2d 304 (D. Mass. 2013); Mwani v. Laden, 947 F. Supp. 2d 1 (D.D.C. 2013). For interesting analyses of *Kiobel* see generally Sarah H. Cleveland, *After* Kiobel, 12 J. INT'L CRIM. JUST. 551 (2014); Louise Weinberg, *What We Don't Talk About When We Talk About Extraterritoriality:* Kiobel *and the Conflict of Laws*, 99 CORNELL L. REV. 1471 (2014).

10. *See* Ruggie, *Clarifying the Concepts*, *supra* note 1, para. 29 (stating that the more than forty cases brought under the ATS constitute the "largest body of domestic jurisprudence regarding corporate responsibility for violations of international law").

11. 3 INT'L COMM'N OF JURISTS, *supra* note 1, at 6; Ruggie, *Clarifying the Concepts*, *supra* note 1, para. 29.

12. Prosecutor v. Perišić, Case No. IT-04-81-A, Appeals Judgement, para. 44 (Int'l Crim. Trib. for the Former Yugoslavia Feb. 28, 2013).

Jurisprudence stemming from these three different contexts has in common that all courts feel the need to limit liability for acts of assistance that consist of an ordinary commercial transaction, or a dual-purpose act, by requiring either that the assistance reach a certain significance threshold (limitations at the actus reus level of liability), or that the mental state with which it was carried out make the assistance particularly reprehensible (limitations at the mens rea level of liability). In the particular context of corporate complicity liability in human rights violations, academic debate of liability standards largely focuses on whether the relevant mens rea standard should be one of purpose or one of knowledge.[13] While clearly important, this Article goes beyond this question and argues that the mens rea standard cannot be understood and determined in isolation. Without taking a look at all elements of liability and their interaction, it is not possible to sufficiently understand the concerns that led to stricter limitations of complicity liability through adopting a purpose standard of mens rea, or to appreciate fully the implications of this approach. In light of a holistic discussion of the interplay of the various elements of complicity liability, this Article will show that the fear that without a mens rea standard of purpose, corporate complicity liability might be limitless is unjustified, and that better alternatives to restricting liability exist.

When referring to complicity, this Article understands it to be synonymous with aiding and abetting, the main form of participation in which the central question of this Article arises, namely whether and under what circumstances ordinary commercial activities can give rise to liability for human rights violations committed by third parties. To talk about corporate complicity in general terms might seem to imply that this is a uniform concept. This, however, is not the case, and context is crucial when refining the criteria to be applied in any given scenario. Legal complicity liability might require stricter limitations and allow for less flexibility than liability under soft law instruments. Criminal liability partly serves different functions, and has different consequences, from civil complicity liability,[14] which might need to be reflected in the nuances of the criteria to be applied. The legal context of the jurisdiction in which liability is established is also of crucial importance. It will also make a difference whether liability is determined retrospectively, in order to give rise to compensation or punishment, or looked at prospectively in order to fulfill due diligence responsibilities.

---

13. *See generally* Shriram Bhashyam, *Knowledge or Purpose? The Khulumani Litigation and the Standard for Aiding and Abetting Liability under the Alien Tort Claims Act*, 30 CARDOZO L. REV. 245 (2008); Doug Cassel, *Corporate Aiding and Abetting of Human Rights Violations: Confusion in the Courts*, 6 NW. J. INT'L HUM. RTS. 304 (2008); Bryan Cox, Comment, *Confused Intent: A Critique of the Fourth Circuit's Adoption of a Purpose Mens Rea Standard for Aiding and Abetting Liability under the Alien Tort Statute [*Aziz v. Alcolac, Inc.*, 658 F.3d 388 (4th Cir. 2011)]*, 51 WASHBURN L.J. 705 (2012); Sabine Michalowski, *The* Mens Rea *Standard for Corporate Aiding and Abetting Liability – Conclusions from International Criminal Law*, 18 UCLA J. INT'L L. & FOREIGN AFF. 237 (2014) [hereinafter Michalowski, *The Mens Rea Standard*]; David Scheffer & Caroline Kaeb, *The Five Levels of CSR Compliance: The Resiliency of Corporate Liability under the Alien Tort Statute and the Case for a Counterattack Strategy in Compliance Theory*, 29 BERKELEY J. INT'L L. 334 (2011); Angela Walker, *The Hidden Flaw in* Kiobel: *Under the Alien Tort Statute the* Mens Rea *Standard for Corporate Aiding and Abetting is Knowledge*, 10 NW. J. INT'L HUM. RTS. 119 (2011).

14. *See* Nathan Isaac Combs, Note, *Civil Aiding and Abetting Liability*, 58 VAND. L. REV. 241, 250–53 (2005) (discussing different purposes of criminal and tort law); James G. Stewart, *A Pragmatic Critique of Corporate Criminal Theory: Lessons from the Extremity*, 16 NEW CRIM. L. REV. 261, 281–89 (2013) (discussing the practical distinction between corporate civil and criminal liability).

In light of these considerations, the purpose of the discussion that follows is not and cannot be to present detailed liability criteria that will work equally in all contexts. Rather, it will serve the more modest aim of analyzing and drawing conclusions from the implications of different approaches to determining the necessary actus reus and mens rea elements of corporate complicity liability, while recognizing that the details need to be developed with reference to the specific context in which the question of corporate complicity liability arises. Nevertheless, while the exact legal definitions of complicity as well as the applicable liability standards differ from State to State, this Article will show that the broad policy considerations that influence how to address the issue are not specific to any particular jurisdiction or context. Indeed, the international nature of the problem is reflected in the many efforts at the international level to define corporate complicity and to develop standards for corporate human rights responsibilities.[15]

I. THE U.S. COURTS' APPROACH TO CORPORATE COMPLICITY LIABILITY UNDER THE ALIEN TORT STATUTE

Given that complicity liability requires both an actus reus and a mens rea,[16] liability criteria need to define both the relevant act of assistance and the necessary mental element. At the objective level, the liability standard determines what effect the corporate activity must have on the commission of the offense, including how close the causal link between the act of assistance and the offense committed by the principal needs to be, to justify the imposition of secondary liability on the corporation. Thus, the actus reus standard defines whether, for example, in a given case the sale of military vehicles to a regime that uses them to carry out extrajudicial killings qualifies as an act of aiding and abetting this violation. The mens rea standard defines the state of mind with which the corporation must have provided the assistance in order to incur liability. In the example of the sale of military vehicles, the question asked at this level would be whether liability requires that the corporation acted with knowledge that the sale would further these violations, with the desire of facilitating them, or with some other mental state. These two components of aiding and abetting liability thus restrict the liability of the accomplice in different ways.

As the relevant liability standards provide the tool for determining whether an act is lawful or gives rise to complicity liability, their definition raises important policy issues regarding the limits of lawful commercial activities and the scope of corporate complicity liability.

15. *See generally, e.g.*, 3 INT'L COMM'N OF JURISTS, *supra* note 1; *Global Compact Principle Two*, UNITED NATIONS GLOBAL COMPACT (last updated Jan. 14, 2015), http://www.unglobalcompact.org/AboutTheGC/TheTenPrinciples/index.html; Ruggie, *Clarifying the Concepts*, *supra* note 1.

16. Prosecutor v. Taylor, Case No. SCSL-03-01-A, Appeals Judgment, paras. 346–47 (Int'l Crim. Trib. for the Former Yugoslavia Sept. 26, 2013).

A. Restricting Corporate Complicity Liability at the Actus Reus Level

The standard actus reus test in U.S. ATS aiding-and-abetting cases, drawn from international criminal law,[17] is that of practical assistance, encouragement, or moral support which has a substantial effect on the perpetration of the crime.[18] Thus, not every act of assistance is sufficient to form the actus reus of aiding and abetting. Rather, the act must have an effect on the commission of the principal offense, and a substantial effect at that. Assistance having a substantial effect "need not constitute an indispensable element, that is, a *conditio sine qua non* for the acts of the principal."[19] "An accessory may be found liable even if the crimes could have been carried out through different means or with the assistance of another."[20]

How to apply this test in corporate complicity cases and decide under what circumstances commercial acts have a substantial effect on the commission of human rights violations by third parties is a difficult task which only very few courts in ATS cases have taken up, an exception being the district court decision in In re *South African Apartheid Litigation.*[21] The case arose from claims by South African victims' groups against several multinational corporations, including banks, automobile manufacturers, and information technology firms,[22] for aiding and abetting crimes committed by the South African apartheid regime.[23] When the case reached the district court for the second time in 2009, the court discussed in detail how to determine whether an act had a substantial effect on the commission of gross human rights violations. The court started its analysis of this issue by suggesting that:

> It is (or should be) undisputed that simply doing business with a state or individual who violates the law of nations is insufficient to create liability under customary international law. International law does not impose liability for declining to boycott a pariah state or to shun a war criminal.

---

17. *See, e.g.*, Prosecutor v. Furundžija, Case No. IT-95-17/1-T, Judgement, para. 235 (Int'l Crim. Trib. for the Former Yugoslavia Dec. 10, 1998) (finding that actus reus requires "practical assistance, encouragement, or moral support which has a substantial effect on the perpetration of the crime"); Prosecutor v. Du[ko] Tadi (Prosecutor v. Tadić), Case No. IT-94-1-T, Opinion and Judgement, para. 688 (Int'l Crim. Trib. for the Former Yugoslavia May 7, 1997) (requiring the act to have a substantial effect on the illegal act); Prosecutor v. Blagojević & Jokić, Case No. IT-02-60-A, Appeal Judgement, paras. 127, 134 (Int'l Crim. Trib. for the Former Yugoslavia May 9, 2007) (observing that substantial effect is a "fact-based inquiry"); United States v. von Weizsaecker (The Ministries Case), 14 TRIALS OF WAR CRIMINALS 478 (1950) ("The question is whether they knew of the program and whether in any substantial manner they aided, abetted, or implemented it.").

18. *In re* Chiquita Brands Int'l, Inc., 792 F. Supp. 2d 1301, 1350 (S.D. Fla. 2011); Presbyterian Church of Sudan v. Talisman Energy, Inc., 582 F.3d 244, 258 (2d Cir. 2009); Khulumani v. Barclay Nat'l Bank, Ltd., 504 F.3d 254, 277 (2d Cir. 2007) (Katzmann, J., dissenting); Doe I v. Unocal Corp., 395 F.3d 932, 951 (9th Cir. 2002).

19. *Furundžija*, Case No. IT-95-17/1-T, para. 209.

20. *In re* S. African Apartheid Litig., 617 F. Supp. 2d 228, 258 (S.D.N.Y. 2009); *accord Tadić*, Case No. IT-94-1-T, para. 688.

21. In re *S. African Apartheid Litig.*, 617 F. Supp. 2d at 257. The last surviving claims in this case were recently dismissed in light of the Supreme Court decision in *Kiobel v. Royal Dutch Petroleum Co.*, 133 S. Ct. 1659 (2013), and its application to the apartheid litigation case by the Second Circuit in *Balintulo v. Daimler AG*, 727 F.3d 174 (2d Cir. 2013). *In re* S. African Apartheid Litig., No. 02 MDL 1499(SAS), 2014 WL 4290444 (S.D.N.Y. Aug. 28, 2014).

22. *In re* S. African Apartheid Litig., 346 F. Supp. 2d 538, 542–43 (S.D.N.Y. 2004).

23. *Id.* at 544–45.

> Aiding a criminal "is not the same thing as aiding and abetting [his or her] alleged human rights abuses."[24]

Thus, the provision of goods or services to a State that commits gross human rights violations, or any other commercial dealings with such a State, do not in and of themselves give rise to complicity liability.[25] Some commentators,[26] as well as some of the judges hearing the case at an earlier stage,[27] suggested that the claims in In re *South African Apartheid Litigation* deserved to be dismissed on the basis that the complaints asserted no more than that the defendants had engaged in commerce with the apartheid regime. The District Court, on the other hand, understood the plaintiffs' allegations as arguing that the defendant corporations' activities had a substantial effect on the crimes carried out by the apartheid regime.[28] The court stressed that where this can be demonstrated, liability does not follow from merely doing business with the regime, or from aiding and abetting the regime as such, but rather from the fact that the corporation aided and abetted the violations committed by the regime.[29]

This conclusion made it necessary to engage with the question of how to determine whether a commercial activity has a substantial effect on gross human rights violations. The court sought recourse in Nuremberg case law to answer this question,[30] even though the 'substantial effect' formula was not used by Nuremberg tribunals but was rather developed many years later by the International Criminal Tribunal for the Former Yugoslavia.[31] In the *Ministries Case*,[32] the Nuremberg Tribunal acquitted Karl Rasche, a member of the board of managers of Dresdner Bank during the Nazi period, because:

> A bank sells money or credit in the same manner as the merchandiser of any other commodity.... Loans or sale of commodities to be used in an unlawful enterprise may well be condemned from a moral standpoint and

---

24. In re *S. African Apartheid Litig.*, 617 F. Supp. 2d at 257 (citing Mastafa v. Australian Wheat Bd., No. 07 Civ. 7955(GEL), 2008 WL 4378443 (S.D.N.Y. Sept. 25, 2008)).

25. *Id.*

26. Michael D. Ramsey, *International Law Limits on Investor Liability in Human Rights Litigation*, 50 HARV. INT'L L.J. 271, 280 (2009) (observing that some of the claims seemed to rest on "little more than allegations that the defendants' operations aided the South African economy").

27. In re *S. African Apartheid Litig.*, 346 F. Supp. 2d at 551; *see also* Khulumani v. Barclay Nat'l Bank, Ltd., 504 F.3d 254, 293–94 (2d Cir. 2007) (Korman, J., dissenting in part) ("Thus, car companies are accused of selling cars, computer companies are accused of selling computers, banks are accused of lending money, oil companies are accused of selling oil, and pharmaceutical companies are accused of selling drugs.").

28. *See* In re *S. African Apartheid Litig.*, 617 F. Supp. 2d at 257–59 (discussing the application of the "substantial assistance" standard in the context of commerce with human rights violators).

29. *Id.*; *see also Khulumani*, 504 F.3d at 289 (Hall, J., concurring) (arguing for extending liability in "cases in which a defendant played a knowing and substantial role in the violation of a clearly recognized international law norm").

30. In re *S. African Apartheid Litig.*, 617 F. Supp. 2d at 258.

31. *See* Prosecutor v. Furundžija, Case No. IT-95-17/1-T, Judgement, paras. 245, 249 (Int'l Crim. Trib. for the Former Yugoslavia Dec. 10, 1998) (applying the "substantial effect" test by the International Criminal Tribunal for the Former Yugoslavia (ICTY)).

32. United States v. von Weizsaecker ("The Ministries Case"), 14 TRIALS OF WAR CRIMINALS 308 (1950).

> reflect no credit on the part of the lender or seller in either case, but the transaction can hardly be said to be a crime.[33]

In the *Zyklon B Case*, on the other hand, Bruno Tesch, whose factory had manufactured and sold the lethal gas that was used in Nazi concentration camps, was found guilty of aiding and abetting crimes against humanity for supplying the gas used to execute allied nationals.[34] For the court in In re *South African Apartheid Litigation*, the different outcomes in the two cases rest on:

> [T]he quality of the assistance provided to the primary violator. Money is a fungible resource, as are building materials. However, poison gas is a killing agent, the means by which a violation of the law of nations was committed. The provision of goods specifically designed to kill, to inflict pain, or to cause other injuries resulting from violations of customary international law bear a closer causal connection to the principal crime than the sale of raw materials or the provision of loans.[35]

This led the court to the conclusion that, in the context of the provision of commercial goods or services, it is sufficient, but also necessary, that the aider and abettor provide the means by which a violation of the law is carried out.[36]

Based on this definition, the court found the actus reus of aiding and abetting the crime of apartheid to be established regarding the allegation that "IBM and Fujitsu supplied computer equipment designed to track and monitor civilians with the purpose of enforcing the racist, oppressive laws of apartheid" as well as the software and hardware to run the system "used to track racial classification and movement for security purposes."[37] These acts were essential for "implementing and enforcing the racial pass laws and other structural underpinnings of the apartheid system"[38] and constituted "the means by which the South African Government carried out both racial segregation and discrimination."[39]

However, the court rejected the idea that "the mere sale of computers to the Department of Prisons—despite the widely held knowledge that political prisoners were routinely held and tortured without trial— . . . constitute[d] substantial assistance to that torture."[40] Equally, with regard to the allegation that IBM had supplied computers to armaments manufacturers that were crucial to the South African Defense Forces, the court suggested that "the sale of equipment used to enhance the logistics capabilities of an arms manufacturer is not the same thing as selling arms used to carry out extrajudicial killing; it is merely doing business with a bad actor."[41]

---

33. *Id.* at 622.

34. The Zyklon B Case, 1 LAW REPORTS OF TRIALS OF WAR CRIMINALS 93, 101–02 (1947).

35. In re *S. African Apartheid Litig.*, 617 F. Supp. 2d at 258.

36. *See id.* at 258–59 (premising liability on the provision of the means by which a crime is committed, which is sufficient to meet the actus reus requirement).

37. *Id.* at 268 (internal quotations omitted).

38. *Id.*

39. *Id.*

40. *Id.*

41. In re *S. African Apartheid Litig.*, 617 F. Supp. 2d at 268–69.

When analyzing the claims against the automotive defendants, the court was satisfied that the sale of "heavy trucks, armored personnel carriers, and other specialized vehicles to the South African Defense Forces and . . . the South African police unit charged with investigating anti-apartheid groups"[42] was sufficient to establish the actus reus of aiding and abetting extrajudicial killings.[43] This was because "[t]hese vehicles were the means by which security forces carried out attacks on protesting civilians and other antiapartheid activists; thus by providing such vehicles to the South African Government, the automotive companies substantially assisted extrajudicial killing."[44] However, allegations that Ford and General Motors sold cars and trucks to the South African police and military forces, and continued to do so after export restrictions were imposed, were insufficient to support a claim because the particular vehicles "without military customization or similar features that link[ed] them to an illegal use" and were "simply too similar to ordinary vehicle sales."[45]

It becomes clear that the court's approach to the actus reus was motivated by a wish to limit complicity liability for ordinary sales and the provision of ordinary commercial services. The question of the substantial effect of the act of assistance on the commission of the violations was approached by focusing on the inherent quality of the products and on whether they provided the direct means for the relevant violations. Where this was not the case, the court refrained from any analysis of the use the regime would make of the goods, and of the effect of the sale on the violations. As, for example, computers and computer programs were not the direct means of committing torture, no further analysis of the link between the technology and the violations to assess whether its provision had a substantial effect on their commission was carried out.[46] Consequently, in practice, the conclusion that "[t]he provision of goods specifically designed to kill, to inflict pain, or to cause other injuries resulting from violations of customary international law bear a closer causal connection to the principal crime than the sale of raw materials or the provision of loans,"[47] did not give rise to a heightened analysis of potential causal links in the latter case (e.g., the sale of computers), as the statement might suggest. Rather, the court seems to automatically reject the existence of a causal link in these cases, while automatically assuming such a link in the former scenario (e.g., the sale of poison gas).[48]

The court accordingly excluded as too remote from the commission of the principal offense the provision of goods that are inherently neutral, and which cannot, by their very nature, be the instrument with which violations are carried out. In such cases, no mens rea analysis is necessary as liability already fails at the actus reus/causation stage. On the other hand, supplying goods that are specifically

42. *Id.* at 264.

43. *Id.*

44. *Id.*

45. *Id.* at 267 ("The sale of cars and trucks without military customization or similar features that link them to an illegal use does not meet the *actus reus* requirement of aiding and abetting a violation of the law of nations.").

46. *Id.* at 269.

47. In re *S. African Apartheid Litig.*, 617 F. Supp. 2d at 258.

48. *See id.* at 258–59 (discussing relevance of type of goods provided to whether the actus reus requirement is satisfied).

designed for harmful purposes or that provide the direct means for carrying out gross human rights violations does amount to the actus reus required for complicity liability. In those cases, complicity liability can only be avoided if the defendants acted without the necessary mens rea.

As a mens rea analysis then only becomes necessary where the goods or services provided by the defendant corporation are inherently harmful or specifically designed to assist with the realization of harmful purposes, the mens rea test does not limit liability for neutral or harmless goods or services that were put to detrimental use, but rather restricts liability for the provision of inherently harmful goods or the direct means with which gross human rights violations were committed. The fact that liability is severely restricted at the actus reus level might explain why the court had no problems with adopting a mens rea test of knowledge. The court declared that "[o]ne who substantially assists a violator of the law of nations is equally liable if he or she desires the crime to occur or if he or she knows it will occur and simply does not care."[49] The restrictions placed on the actus reus of aiding and abetting liability are thus counterbalanced by the wide reach of a mens rea standard of knowledge once the actus reus is made out and the corporate activities at issue are shown to go beyond ordinary commercial sales or other ordinary commercial services.[50]

B. Restricting Corporate Complicity Liability at the Mens Rea Level

Many courts that have had to decide corporate complicity cases under the ATS have largely bypassed the actus reus analysis and instead focused their efforts on the mens rea assessment. Regarding the necessary mens rea, the ad hoc international criminal tribunals whose jurisprudence is influential on the approach to liability standards under the ATS apply a knowledge standard;[51] i.e., they require knowledge that these acts assist the commission of the offense. However, the accomplice need not share the principal's wrongful intent.[52] Until October 2009, in line with the jurisprudence of the international criminal tribunals, most U.S. courts adopted a mens rea standard of knowledge that the act of the corporation would assist in the commission of the offense.[53] This changed with the decision in *Presbyterian Church of Sudan v. Talisman Energy, Inc.*,[54] in which the Second Circuit decided that liability for aiding and abetting gross human rights violations under the ATS required that the corporation act with the primary purpose of facilitating the violations, a decision

49. *Id.* at 262.

50. It is worth noting, though, that since the 2009 district court decision in In re *South African Apartheid Litigation*, the Second Circuit has adopted a mens rea standard of purpose, which is therefore now the applicable standard for future decisions. Presbyterian Church of Sudan v. Talisman Energy, Inc., 582 F.3d 244, 247 (2d Cir. 2009).

51. Prosecutor v. Furundžija, Case No. IT-95-17/1-T, Judgement, para. 245 (Int'l Crim. Trib. for the Former Yugoslavia Dec. 10, 1998); Prosecutor v. Vasiljević, Case No. IT-98-32-A, Appeals Judgement, para. 102 (Int'l Crim. Trib. for the Former Yugoslavia Feb. 25, 2004); Prosecutor v. Aleksovski, Case No. IT-95-14/1-A, Judgement, paras. 162–63 (Int'l Crim. Trib. for the Former Yugoslavia Mar. 24, 2000); Prosecutor v. Perišić, Case No. IT-04-81-A, Appeals Judgement, para. 48 (Int'l Crim. Trib. for the Former Yugoslavia Feb. 28, 2013).

52. *Furundžija*, Case No. IT-95-17/1, para. 245.

53. Doe I v. Unocal Corp., 395 F.3d 932, 950–51 (9th Cir. 2002); Cabello v. Fernández-Larios, 402 F.3d 1148, 1157–58 (11th Cir. 2005); *In re* "Agent Orange" Prod. Liab. Litig., 373 F. Supp. 2d 7, 54 (E.D.N.Y. 2005); Almog v. Arab Bank, PLC, 471 F. Supp. 2d 257, 290–91 (E.D.N.Y. 2007).

54. *Talisman*, 582 F.3d at 258–59.

which has since been followed by some federal courts of appeals,[55] while others have confirmed adherence to the knowledge standard.[56]

Even though corporate actors might sometimes knowingly accept that their activities will likely contribute to gross human rights violations that are being carried out, particularly when working in States with poor human rights records, or in the middle of armed conflicts, corporations will only very rarely act with the purpose of facilitating them.[57] Rather, corporate activities will usually primarily be driven by business interests.[58] As a consequence, if corporate responsibility for complicity in gross human rights violations required that the corporation act with the primary purpose of facilitating violations, they would hardly ever be subject to such liability, whereas a mens rea standard of secondary purpose or of knowledge would widen the range of scenarios in which corporations might face complicity charges.[59] The mens rea test to be applied is thus an important, if not in many cases the determinative, factor for defining the scope of corporate complicity liability, as the application of a purpose test will in most cases simply rule out such liability.

The next Part will introduce the reasons behind the switch to a mens rea standard of purpose in corporate complicity cases decided under the ATS, using some recent key cases as examples.

1. *Presbyterian Church of Sudan v. Talisman Energy, Inc.*

In *Talisman*, the plaintiffs alleged that in the course of its oil extraction project in an area of Sudan that was afflicted by a civil war, the defendant built all-weather roads that linked the concession area to military bases.[60] These roads facilitated the oil extraction, but also military activities.[61] The plaintiffs alleged that the roads allowed the military to launch attacks year-round in areas often previously

55. Aziz v. Alcolac, Inc., 658 F.3d 388, 400–01 (4th Cir. 2011).

56. Doe VIII v. Exxon Mobil, 654 F.3d 11, 39 (D.C. Cir. 2011). In *Sarei v. Rio Tinto, PLC*, the Ninth Circuit left open which of the conflicting views on the prevalent mens rea standard under international criminal law it found more convincing, as the court regarded the purpose standard to be met in the case before it. 671 F.3d 736, 765 (9th Cir. 2011) (Schroeder, J., plurality opinion), *vacated*, 133 S. Ct. 1995 (2013).

57. *Cf.* Christoph Burchard, *Ancillary and Neutral Business Contributions to 'Corporate-Political Core Crime': Initial Enquiries Concerning the Rome Statute*, 8 J. INT'L CRIM. JUST. 919, 939 (2010) (assuming that "core criminal policies" are not the primary motivation of business actors); Hans Vest, *Business Leaders and the Modes of Individual Criminal Responsibility under International Law*, 8 J. INT'L CRIM. JUST. 851, 862–63 (2010) [hereinafter Vest, *Business Leaders*] (remarking that with this standard "there seems to be no other alternative than to dismiss most cases involving business leaders, as they will act primarily, or at least simultaneously, for economic purposes").

58. *Cf.* Burchard, *supra* note 57, at 939 (assuming that, in the context of international criminal law, business leaders are frequently influenced by "motives and interests that are incongruent with core criminal policies"); Vest, *Business Leaders*, *supra* note 57, at 855–59.

59. *See, e.g.*, Burchard, *supra* note 57, at 939 (discussing the scope of corporate liability in light of a corporation's purpose and knowledge with regard to an act); Vest, *Business Leaders*, *supra* note 57, at 862–63 ("At least with respect to business leaders who provide the essential means for the commission of war crimes . . . it would hardly seem understandable if 'for the purpose' was not read expansively.").

60. Presbyterian Church of Sudan v. Talisman Energy, Inc., 582 F.3d 244, 249 (2d Cir. 2009).

61. *Id.*

inaccessible due to seasonal flooding.[62] The defendants also upgraded two airstrips in the concessions.[63] This served the purpose of enhancing the safety and convenience of the defendant's personnel, but at the same time supported military activity, as the government used the airstrips to refuel military aircraft, supply troops, take defensive action, and initiate attacks, including regular bombing runs.[64] Security arrangements made for oil company personnel in coordination with the government and military forces resulted, according to the plaintiffs, "in the persecution of civilians living in or near the oil concession areas."[65]

The court highlighted early on that none of the acts the defendant corporation was accused of were "inherently criminal or wrongful."[66] Moreover, "'[t]he activities which the plaintiffs identify as assisting the Government in committing crimes against humanity and war crimes generally accompany any natural resource development business or the creation of any industry.'"[67] Thus, the court regarded this as a case of routine business transactions that were facially lawful. Indeed, the Second Circuit accepted the District Court's assessment in the same case that:

> [T]he plaintiffs' theories of substantial assistance serve essentially as proxies for their contention that Talisman should not have made any investment in the Sudan, knowing as it did that the Government was engaged in the forced eviction of non-Muslim Africans from lands that held promise for the discovery of oil.[68]

In light of such a perception of the complaint, it comes as no surprise that the court looked for ways to reject it. It did so based on a rewriting of the relevant mens rea standard. The court deviated from the vast majority of previous decisions that applied a mens rea standard of knowledge and instead adhered to Judge Katzmann's analysis in *Khulumani*,[69] according to which Nuremberg case law and the Rome Statute of the International Criminal Court demonstrate that the relevant standard for aiding and abetting a violation of international law is that of purpose.[70] Its rejection of the claim then relied on this, it is submitted, mistaken[71] interpretation of international precedent.[72]

---

62. *Id.*

63. *Id.*

64. *Id.* at 249–50.

65. *Id.* at 249.

66. *Talisman*, 582 F.3d at 261.

67. *Id.* at 260–61 (quoting the findings of the district court in the same case).

68. *Id.* at 261 (alteration in original) (quoting the district court's opinion).

69. Khulumani v. Barclay Nat'l Bank, Ltd., 504 F.3d 254, 276–79 (2d Cir. 2007) (Katzmann, J., concurring); *accord id.* at 332–33 (Korman, J., concurring in part, dissenting in part). Judge Hall, on the other hand, pronounced himself in favor of a standard of knowledge in that case, though based on the view that the relevant mens rea standard has to be derived from U.S. federal law. *Id.* at 287–89. Even though two judges thus agreed on a mens rea standard of purpose, Judge Korman did so in his partial dissent, stating that had he reached the issue, he would have supported Judge Katzmann's view with regard to the applicable mens rea test. As a consequence of this split in opinion, the court in *Talisman* did not regard Judge Katzmann's view to set a binding precedent and therefore addressed the question afresh. *Talisman*, 582 F.3d at 258.

70. *Talisman*, 582 F.3d at 258–59.

71. For a critical discussion of the *Talisman* court's understanding of international precedent see generally Michalowski, *The Mens Rea Standard*, *supra* note 13.

72. *See Talisman*, 582 F.3d at 259, 263, 268 (applying purported mens rea standard of purpose in

When considering the corporation's liability with regard to building the all-weather roads and airstrips, the court acknowledged the defendant's awareness of the use made of these facilities by the Sudanese military.[73] Under the knowledge standard of mens rea that was prevalent in U.S. case law on aiding and abetting liability under the ATS prior to *Talisman*,[74] this might have been sufficient to establish the necessary mens rea of aiding and abetting liability. However, under the newly introduced mens rea standard of purpose, awareness was not decisive and the court found it necessary to undertake an analysis of the purpose with which the activities of the corporation had been carried out.[75] It attached significance to the fact that all-weather roads and airstrips were necessary for developing an oil-extraction project in a remote location.[76] This meant that there were, therefore, "benign and constructive purposes for these projects, and (more to the point) there [was] no evidence that any of this was done for an improper purpose."[77] The court further clarified that:

> Even if Talisman built roads or improved the airstrips with the intention that the military would also be accommodated, GNPOC had a legitimate need to rely on the military for defense. It is undisputed that oil workers in that tumultuous region were subjected to attacks: rebel groups viewed oil installations and oil workers as enemy targets; . . . rebels launched a nighttime mortar attack against a Heglig camp where 700 oil workers were living; and in Block 5A the attacks caused that concessionaire (Lundin Oil AB) to close down operations for an extended period. In these circumstances, evidence that GNPOC was coordinating with the military supports no inference of a purpose to aid atrocities.[78]

Thus, given the mens rea requirement of purpose, to knowingly assist gross human rights violations carried out by a government would not result in corporate liability as long as the corporation was not motivated by an improper desire to bring about these violations but rather acted in pursuit of a legitimate purpose or interest, such as the defense of its activities against rebel attacks, or more generally the desire to guarantee the smooth and safe running of its business operations. Indeed, the court understood the mens rea test of purpose as requiring that the act of assistance be directly motivated by the wish to bring about atrocities and that this, moreover, constitute the primary reason for the act.[79] Purpose thus seems to be synonymous with motive.

The plaintiffs had deduced the corporation's awareness of the effect of its acts of assistance on the gross human rights violations carried out by Sudanese forces

---

dismissing plaintiffs' claim).

73. *Id.* at 262.

74. *See, e.g.*, Doe VIII v. Exxon Mobil, 654 F.3d 11, 39 (D.C. Cir. 2011) (applying a knowledge standard for mens rea for the ATS under customary international law).

75. *Talisman*, 582 F.3d at 263–64.

76. *Id.*

77. *Id.* at 262.

78. *Id.*

79. *See id.* at 263 (stating that the defendants must act with the purpose to assist the international law violations).

from the fact that senior Talisman officials had protested against the government's use of their infrastructure, and from their possession of security reports that expressed concern about the use of airstrips by the military.[80] However, the court held not only that knowledge was insufficient to establish the mens rea but that this "evidence of knowledge (and protest) cuts against Talisman's liability."[81] This was because such a protest indicated the corporation's opposition to the violations and therefore negated any inference of a desire to facilitate them.[82] The court concluded that:

> There is evidence that southern Sudanese were subjected to attacks by the Government, that those attacks facilitated the oil enterprise, and that the Government's stream of oil revenue enhanced the military capabilities used to persecute its enemies. But if ATS liability could be established by knowledge of those abuses coupled only with such commercial activities as resource development, the statute would act as a vehicle for private parties to impose embargos or international sanctions through civil actions in United States courts. Such measures are not the province of private parties but are, instead, properly reserved to governments and multinational organizations.[83]

This is in line with Judge Sprizzo's view in In re *South African Apartheid Litigation*, which regarded it to be relevant in the context of considering corporate liability that the U.S. government, "consistent with most other world powers, supported and encouraged business investment in apartheid South Africa" and opted for a policy of constructive engagement, relying on "the tool of economic investment as a means to achieve greater respect for human rights and a reduction in poverty in developing countries."[84] He moreover pointed out that:

> In a world where many countries may fall considerably short of ideal economic, political, and social conditions, this Court must be extremely cautious in permitting suits here based upon a corporation's doing business in countries with less than stellar human rights records, especially since the consequences of such an approach could have significant, if not disastrous, effects on international commerce.[85]

While Judge Sprizzo relied on these considerations to reject corporate aiding and abetting liability altogether, the court in *Talisman* used them to justify the need for a restrictive mens rea test of purpose as the only way to effectively limit liability. Without a thorough actus reus assessment, it is not clear whether the court thought that most routine business transactions, including the ones at issue in the *Talisman* case, could potentially amount to relevant acts of aiding and abetting human rights violations, or if the imposition of liability was only justified where, in addition to assistance that has a substantial effect on human rights violations, the corporation

80. *Id.* at 262.
81. *Talisman*, 582 F.3d at 262
82. *See id.* (discussing the significance of Talisman's knowledge).
83. *Id.* at 264.
84. *In re* S. African Apartheid Litig., 346 F. Supp. 2d 538, 554 (S.D.N.Y. 2004).
85. *Id.*

acted with more than knowledge. An alternative interpretation might be that the court, while doubting that in such cases even the actus reus requirement would be satisfied, adopted the view that it was easier and more effective to restrict liability at the mens rea level, thereby bypassing all discussions of the potential effect of commercial activities on human rights violations that would otherwise be necessary. Indeed, the court's actus reus analysis is largely inconclusive. On the one hand, the Second Circuit seems to approve of the district court's negative view that there was not even a relevant act of substantial assistance.[86] At the same time, it accepts that Talisman's various activities that were at issue in this case had assisted the government,[87] without, however, undertaking any analysis as to whether these acts would amount to practical assistance that had a substantial effect.

Whatever the court's views on whether the actus reus requirement was met in this case, the decision in *Talisman* clearly rests decisively on the court's assessment of the corporation's mens rea. The court's approach demonstrates its view that even acts that have a substantial effect on violations of human rights carried out by others should be shielded from complicity liability unless the corporation had the desire to facilitate these, rather than simply knowingly accepting their occurrence as a side effect of pursuing their business interests.

2. *Kiobel v. Royal Dutch Petroleum Co.* (concurring opinion)

The *Talisman* ruling was cited with approval by Judge Leval in his concurring opinion in *Kiobel*.[88] The main importance of the Second Circuit decision in *Kiobel* clearly lies in the majority holding that international law does not recognize civil liability of corporations for aiding and abetting violations of the law of nations, and that therefore claims based on corporate complicity cannot succeed under the ATS.[89] However, Judge Leval's concurring opinion, while of crucial importance regarding its meticulous rejection of the majority's approach to rejecting corporate liability under international law, at the same time demonstrates that even if such liability were accepted, a mens rea standard of purpose would shield corporations from liability in a great number of scenarios.

In *Kiobel*, the defendant corporations had for several decades been engaged in oil exploration and production in the Ogoni region of Nigeria.[90] According to the plaintiffs, in response to protests by groups of local citizens against adverse effects of the oil operations, the defendant resorted to the Nigerian government to suppress the Ogoni resistance.[91] The most important allegations were that:

> Throughout 1993 and 1994, Nigerian military forces . . . shot and killed Ogoni residents and attacked Ogoni villages—beating, raping, and arresting residents and destroying or looting property—with the assistance

86. *Talisman*, 582 F.3d at 262.

87. *Id.*

88. Kiobel v. Royal Dutch Petroleum Co., 621 F.3d 111, 154 (2d Cir. 2010) (Leval, J., concurring in the judgment).

89. *Id.* at 148–49 (majority opinion).

90. *Id.* at 123.

91. *Id.*

> of defendants. Specifically, plaintiffs allege that defendants, *inter alia*, (1) provided transportation to Nigerian forces, (2) allowed their property to be utilized as a staging ground for attacks, (3) provided food for soldiers involved in the attacks, and (4) provided compensation to those soldiers.[92]

The majority in *Kiobel* did not proceed to an analysis of the facts of the case, as it negated any basis for corporate aiding and abetting liability under the ATS.[93] Judge Leval, however, who disagreed on that fundamental point, had to analyze whether the plaintiffs' allegations were sufficient to make out a case of aiding and abetting liability.[94] Following precedent in *Talisman*, Judge Leval stated that it was not enough for the plaintiffs to allege that the defendant corporations had knowingly contributed to human rights violations carried out by officials of the Nigerian government.[95] It rather needed to be shown that they acted "with a purpose of bringing about the abuses."[96] According to him,

> the Complaint fails to allege facts . . . showing a purpose to advance or facilitate human rights abuses. The provision of assistance to the Nigerian military with *knowledge* that the Nigerian military would engage in human rights abuses does not support an inference of a purpose on Shell's part to advance or facilitate human rights abuses. An enterprise engaged in finance may well provide financing to a government, in order to earn profits derived from interest payments, with the knowledge that the government's operations involve infliction of human rights abuses. Possession of such knowledge would not support the inference that the financier acted with a purpose to advance the human rights abuses.[97]

In the scenario painted here, a question might arise with regard to the necessary actus reus, as it would require some detailed analysis to show that providing financing to a government would have a substantial effect on the human rights violations it commits.[98] However, Judge Leval skipped this issue completely and instead concentrated on the mens rea assessment. Applying *Talisman*, he took the position that one cannot infer intent to violate human rights from an act of knowing participation that is primarily motivated by business reasons.[99] As a consequence, as long as the principal purpose of a corporation is making profit, and it is indifferent to whether gross human rights violations are carried out by the government of the state

92. *Id.*

93. *Id.* at 140–41.

94. *See Kiobel*, 621 F.3d at 154 (Leval, J., concurring in the judgment) (discussing the standard to be applied in analyzing whether plaintiff's allegations were sufficient).

95. *Id.* (asserting that purpose standard of mens rea liability applied).

96. *Id.* at 188.

97. *Id.* at 193.

98. For a detailed discussion see generally Sabine Michalowski, *No Complicity Liability for Funding Gross Human Rights Violations?*, 30 BERKELEY J. INT'L L. 451 (2012) [hereinafter Michalowski, *No Complicity Liability*].

99. *See Kiobel*, 621 F.3d at 158 (Leval, J., concurring in the judgment) (explaining how profiting through the mere provision of financing or military equipment for an entity accused of violating human rights will not support an inference that a corporation "acted *with a purpose* to promote or advance those violations" (emphasis in original)).

in which it operates, it can knowingly participate in them without risking complicity liability.

This becomes particularly clear when Judge Leval discusses the allegations that "representatives of Shell and its Nigerian subsidiary met in Europe 'to formulate a strategy to suppress MOSOP [Movement for Survival of Ogoni People] and to return to Ogoniland.'"[100] According to Judge Leval, even "that Shell 'knew' the Nigerian military would use 'military violence against Ogoni civilians' as part of the effort to suppress MOSOP . . . does not support an inference that Shell *intended* for such violence to occur."[101] Thus, to enlist the help of the government in the suppression of the protests, knowing that this would be implemented, at least partly, through measures that involve gross human rights violations would not be sufficient to result in liability for aiding and abetting.

Judge Leval also accepted the argument already advanced in Talisman that it was legitimate for "an entity engaged in petroleum exploration and extraction . . . [to] provide financing and assistance to the local government in order to obtain protection needed for the petroleum operations with knowledge that the government acts abusively in providing the protection."[102] He concluded that there were insufficient allegations of

> facts which support a plausible assertion that Shell rendered assistance to the Nigerian military and police for the purpose of facilitating human rights abuses, as opposed to rendering such assistance *for the purpose* of obtaining protection for its petroleum operations with awareness that Nigerian forces would act abusively. In circumstances where an enterprise requires protection in order to be able to carry out its operations, its provision of assistance to the local government in order to obtain the protection, even with knowledge that the local government will go beyond provision of legitimate protection and will act abusively, does not without more support the inference of a purpose to advance or facilitate the human rights abuses and therefore does not justify the imposition of liability for aiding and abetting those abuses.[103]

The court did not specify what "more" would be necessary to justify the inference of a mens rea of purpose. It becomes clear, though, that purpose is understood as primary purpose—that is, a desire that the human rights violations should occur—instead of indifference to or acceptance of such violations as a consequence of knowing assistance.

Judge Leval invoked policy considerations in favor of a mens rea standard of primary purpose in the context of corporate complicity litigation, his main concern being to find an acceptable way to apportion and restrict liability.[104] In his view, it is the mens rea that limits the extent of corporate liability and delineates the boundaries between legitimate business activities and conduct that gives rise to

100. *Id.* at 192.
101. *Id.*
102. *Id.* at 193.
103. *Id.* at 193–94.
104. *Id.* at 158.

corporate liability,[105] and only a purpose standard can effectively achieve this aim. He invokes two scenarios to show the, in his view undesirable, consequences of applying a knowledge standard. The first is that of "corporations engaged in the extraction of precious resources in remote places . . . [which] will contribute money and resources to the local government to help it render the protection the corporation needs for its operations"[106] and that are sued for aiding and abetting if the government troops then commit atrocities. The second case is that of "[t]he shoemaker who makes Hitler's shoes [who] should not be held responsible for Hitler's atrocities, even if the shoemaker knows that a pair of shoes will help Hitler accomplish his horrendous agenda."[107] It seems as if for Judge Leval, Hitler's shoemaker is in the same league as "business corporations engaged in finance or in the sale of food or military supplies [which] might raise funds for, or sell supplies to, a government that is known to violate the law of nations."[108] Both examples refer to cases of "profit-motivated provision of finance or supplies, done with awareness of the purchasing government's record of atrocities."[109]

> [An] imposition of liability . . . would go too far in impeding legitimate business, by making a business corporation responsible for the illegal conduct of local government authorities that is beyond the corporation's control, and which the corporation may even deplore. . . . Concerns of this nature might well give pause to a court contemplating the imposition of liability on a business corporation for aiding and abetting in a government's infliction of human rights abuses, where the corporation did not promote, solicit, or desire the violation of human rights.[110]

Judge Leval made these observations in the context of a concurring opinion that makes a forceful plea in favor of preserving the possibility of suing corporations under the ATS for their complicity in human rights violations. It would thus be possible to interpret his discussion as an attempt to alleviate concerns that the existence of such causes of action would lead to limitless corporate liability by showing that the purpose test sets clear restrictions on such liability. Nevertheless, in uncritically applying the purpose test to these cases and justifying it based on the policy considerations discussed above, his approach, just like that adopted in *Talisman*, suggests that as long as the facilitation of human rights violations is just a byproduct of business motivated decisions, it should not result in liability. He seems to regard even their direct furtherance as legitimate as long as the reasons for that furtherance are business related, including guaranteeing the safety of business operations and personnel.[111]

---

105. *See Kiobel*, 621 F.3d at 158 (Leval, J., concurring in the judgment) (asserting that the court "will not support the imposition of aiding and abetting liability on the corporation for that government's abuses unless the corporation acted *with a purpose* to promote or advance those violations").

106. *Id.* at 157.

107. *Id.* at 158.

108. *Id.* at 157.

109. *Id.*

110. *Id.* at 158.

111. *Kiobel*, 621 F.3d at 158 (Leval, J., concurring in the judgment).

His observation that liability should not attach for illegal conduct of the business partner that is beyond the corporation's control[112] is interesting. Unfortunately, it is not further explored, and whether and how the purpose test might address this issue therefore is not made clear. Neither is it evident why promoting and soliciting human rights violations is mentioned in the same breath as desiring them, as the first two scenarios seem to refer to the actus reus, while the last is clearly a mens rea element.

3. *Doe v. Nestle*

In *Doe v. Nestle*, victims of child slavery who were forced to work on cocoa plantations in the Ivory Coast brought an aiding and abetting case against corporations that control the production of Ivorian cocoa.[113] The plaintiffs alleged that the "defendants operate in the Ivory Coast 'with the unilateral goal of finding the cheapest sources of cocoa.'"[114] According to the plaintiffs, even though they were well aware of the child slavery problem in the Ivory Coast (through first-hand knowledge acquired during their numerous visits to Ivorian farms, and through the reports of domestic and international organizations),[115] they "continue[d] to supply money, equipment, and training to Ivorian farmers, knowing that these provisions [would] facilitate the use of forced child labor."[116] In the United States, the defendants also lobbied against efforts to curb the use of child slave labor by requiring importers and manufacturers to certify their products as "slave free."[117]

When discussing whether or not these allegations were sufficient to meet the mens rea requirement for corporate aiding and abetting under the ATS, the court left open whether or not the necessary standard was one of purpose or knowledge, as it found that plaintiffs' factual allegations met the requirements of the purpose test.[118] While the purpose standard would not be "satisfied merely because the defendants intended to profit by doing business in the Ivory Coast,"[119] an inference of purpose could be based on allegations that the corporation did not use their control over the Ivory Coast cocoa market to stop "the use of child slave labor by their suppliers."[120] This, coupled with the cost-cutting benefit they allegedly received from the use of child slaves, justified the inference that the defendants acted with purpose.[121] The defendants' alleged lobbying efforts against legislative labeling requirements were regarded as corroborating the inference that they acted with the purpose of facilitating slave labor.[122]

---

112. *Id.*
113. Doe I v. Nestle USA, Inc., 766 F.3d 1013, 1017–18 (9th Cir. 2014).
114. *Id.* at 1017.
115. *Id.*
116. *Id.*
117. *Id.*
118. *Id.* at 1024.
119. *Nestle*, 766 F.3d at 1025.
120. *Id.*
121. *Id.*
122. *Id.*

The court distinguished this case from *Talisman* where the defendant did not "in any way benefit from the underlying human rights atrocities carried out by the Sudanese military, and in fact, those atrocities ran contrary to the defendant's goals in the area, and even forced the defendant to abandon its operations."[123] In *Nestle,* the corporation "profited by doing business with known human rights violators . . . [and] sought to accomplish their own goals by supporting violations of international law."[124] It did not matter that the plaintiffs in *Nestle* "conceded that the defendants did not have the subjective motive to harm children," that instead, "the defendants' motive was finding cheap sources of cocoa" and that there was "no allegation that the defendants supported child slavery due to an interest in harming children in West Africa."[125] Thus, the court concluded that "the defendants sought a legitimate goal, profit, through illegitimate means, purposefully supporting child slavery."[126]

4. *Sarei v. Rio Tinto*

Sarei v. Rio Tinto is another case where a court left open whether the relevant mens rea standard was one of knowledge or of purpose, as it found that the purpose standard had been met.[127] In that case, the majority opinion suggested that in order to satisfy the mens rea standard of purpose it was sufficient to allege that the defendant corporation

> issued the PNG government "an ultimatum": displace the local residents interfering with its mining operations, no matter the means, or Rio would abandon all investments on PNG. When the PNG government employed military means to fulfill Rio's demands, Plaintiffs allege, Rio provided the PNG military helicopters and vehicles to carry out the operations, even after reports of war crimes became public. When initial efforts were insufficient to displace the locals, PNG imposed a blockade on Bougainville; Plaintiffs allege that at a meeting "between PNG officials and two top Rio executives, one top Rio manager encouraged continuation of the blockade to 'starve the bastards out . . . .'" Moreover, Rio allegedly assured the PNG government that the continued maintenance of the blockade was enough to prevent Rio from withdrawing from PNG, while Rio simultaneously attempted to repress reporting of the humanitarian crisis unfolding on the island. These allegations support much more than "an inference of mere knowledge on Rio Tinto's part," it supports an inference that Rio Tinto actively *encouraged* the killing of Bougainvilleans.[128]

123. *Id.* at 1024.

124. *Id.*

125. *Nestle*, 766 F.3d at 1025.

126. *Id.* at 1025–26.

127. *See* Sarei v. Rio Tinto, PLC, 671 F.3d 736, 765–67 (9th Cir. 2011) (Schroeder, J., plurality opinion), *vacated*, 133 S. Ct. 1995 (2013) ("Because plaintiffs allege that Rio Tinto specifically intended to harm them in aiding and abetting the commission of war crimes, we need not decide whether the broader interpretation of 'purpose' [which is inferred from the knowledge of likely consequences] would also sustain liability . . . .").

128. *Id.* at 766 (citations omitted). Judge Leval indicated in *Kiobel* that he would agree to a finding of

According to the court, these were sufficient factual allegations to support a claim that "Rio Tinto specifically intended to harm the residents of Bougainville."[129] It seems crucial for a finding of liability under the purpose test that the corporation expressly incited the government's commission of gross human rights violations in order to protect its business interests, instead of simply knowing and accepting that such violations might occur. This is so even though encouragement seems to be an actus reus rather than a mens rea element of complicity liability.

5. In re *Chiquita Brands*

Another case in which a court found that a corporation had acted with a mens rea of purpose is In re *Chiquita Brands*.[130] An action was filed by "family members of trade unionists, banana-plantation workers, political organizers, social activists, and others tortured and killed by the Autodefensas Unidas de Colombia (AUC), a paramilitary organization operating in Colombia," against Chiquita for aiding and abetting the crimes committed by the AUC.[131] According to the court and based on admissions made by Chiquita itself:

> Chiquita formed an agreement with the AUC, paying them to pacify the banana plantations and to suppress union activity. In return for Chiquita's support, the AUC agreed it would drive the guerrillas out of Chiquita's banana-growing areas and maintain a sufficient presence to prevent the guerrillas from returning. Furthermore, the AUC would provide Chiquita with security, labor quiescence, and ensure that the unions were not infiltrated by leftists sympathetic to the FARC or ELN guerrillas. This arrangement benefitted Chiquita, as labor unrest and strikes were minimized while profits increased.[132]

The plaintiffs also alleged that Chiquita assisted the AUC by facilitating arms shipments.[133]

The court clarified, in line with *Talisman*, that allegations of mere knowledge that the AUC would commit such offenses were insufficient. Rather, the plaintiffs needed to plead that "Chiquita paid the AUC with the specific purpose that the AUC commit the international-law offenses alleged in the complaints," which had to allege that "Chiquita intended for the AUC to torture and kill civilians in Colombia's banana-growing regions."[134] The Court found this test to be satisfied, for example, with regard to the allegations that:

> Chiquita supported terrorist groups in Colombia by paying them and assisting them to obtain arms and smuggle drugs. Chiquita knew that these

purpose on the basis of such facts. Kiobel v. Royal Dutch Petroleum Co., 621 F.3d 111, 158 (2d Cir. 2010) (Leval, J., concurring in the judgment).

129. *Rio Tinto*, 671 F.3d at 766.

130. *In re* Chiquita Brands Int'l, Inc., 792 F. Supp. 2d 1301, 1351–52 (S.D. Fla. 2011).

131. *Id.* at 1305.

132. *Id.* at 1309 (citations omitted).

133. *Id.* at 1310.

134. *Id.* at 1344–45.

> groups used illegal violence against civilians and intended that they employ this strategy to quell social and labor unrest in the Northeast Colombian region of Uraba and safeguard the stability and profitability of Chiquita's enterprises in Colombia. . . . Chiquita's acts of assistance to the AUC were made with the intent that the AUC continue carrying out acts of killing, torture, and other illegal violence against the civilian population of Uraba in accordance with the AUC's strategy for suppressing the FARC and deterring its sympathizers. In exchange for its financial support to the AUC, Chiquita was able to operate in an environment in which labor and community opposition was suppressed. . . . Chiquita intended that the AUC continue carrying out acts of killing, torture, and other illegal violence against the civilian population of Uraba in accordance with the AUC's strategy for suppressing the FARC and deterring its sympathizers. In providing the AUC with money and assistance with their arms and drug trafficking, Defendants intended that the AUC obtain arms and continue their practice of killing civilians, especially those civilians who were perceived as threats to the profitability of the banana industry. The leadership of the AUC did, in fact, carry out killings of union members, social organizers and other undesirable groups, as well as civilians with no known or suspected ties to the guerrillas, knowing that Chiquita expected and intended that they do so using the arms and money provided by Chiquita.[135]

The court even held that the defendants had the necessary mens rea for aiding and abetting a war crime, that is "the alleged offenses be carried out in furtherance of a conflict [such that] . . . Chiquita shared the principal's same purpose, i.e., to torture and kill as a means to defeat militarily its enemy."[136] In this respect, the court stressed that "[t]he fact that Chiquita may not have had a military objective of its own, or that it was motivated by financial gain, is not dispositive. A 'lack of motive does not negate intent to assist the underlying acts that may be war crimes.'"[137] Quoting *Drummond II*,[138] the court opined that if it was required that defendants act

> in direct furtherance of a 'military objective' . . . an ATS action would not lie where defendants were motivated by ideology or the prospect of financial gain, as plaintiffs allege here. Indeed under defendants' proposed rule, it is arguable that nobody who receives a paycheck would ever be liable for war crimes.[139]

Applying this reasoning to the case before it, the court then held that:

> The complaints' allegations that Chiquita assisted the AUC with the intent that the AUC's interests were furthered over the FARCs [sic] in the Colombian civil war sufficiently allege the *mens rea* for aiding and abetting

135. *Id.* at 1345–46.

136. *Chiquita Brands Int'l*, 792 F. Supp. 2d at 1348.

137. *Id.* at 1349 (quoting Doe v. Drummond Co. (Drummond II), No. 2:09–CV–01041–RDP, 2010 WL 9450019, at *13 (N.D. Ala. Apr. 30, 2010)).

138. *Drummond II*, 2010 WL 9450019, at *13.

139. *Chiquita Brands Int'l*, 792 F. Supp. 2d at 1349 (quoting *Drummond II*, 2010 WL 9450019, at *13).

> the AUC's war crimes, irrespective of the fact that the company may have chosen the AUC's side for financial, as opposed to military, reasons.[140]

In finding the purpose test to be met even where the corporation was clearly primarily motivated by the wish to further its business interests and not by a desire to facilitate human rights violations, it seems as though, unlike the court in *Talisman*, the court in *Chiquita* did not equate purpose with primary purpose and motive. At the same time, it is very likely that the outcome in *Chiquita* was highly influenced by the fact that the acts of assistance were not regarded as legitimate business activities.

6. Link between the Heightened Mens Rea Standard of Purpose and the Commercial Nature of the Act

In recent years, quite a few courts have moved from a mens rea test of knowledge to one of purpose, motivated by the wish to restrict corporate complicity liability in the context of commercial activities. Indeed, when examining how purpose was defined in these cases and how its existence or absence was established, it becomes clear that the application of the mens rea test was highly influenced by how the courts perceived and characterized the activities which provided the actus reus of aiding and abetting.

In *Talisman* and *Kiobel*, the activities of the defendant corporations, which according to the plaintiffs should be regarded as assisting in gross human rights violations, were classified by the courts as ordinary business activities that pursued a legitimate purpose.[141] To compensate for the facial legitimacy or routine commercial nature of the corporate activities at issue, the courts limited liability to acts that were carried out with a more culpable state of mind than mere knowledge. This approach is based on the assumption that it is legitimate to pursue business interests even where it is clear that the relevant activities substantially assist in human rights violations. Even the direct support of such violations seems to be regarded as legitimate as long as the reasons for such behavior are business-related, which includes guaranteeing the safety of business operations and personnel.[142] *Doe v. Nestle* suggests that an exception to this might be made where the corporation directly benefited from the violations.[143]

This can be contrasted with In re *Chiquita*, where the court clearly did not regard payment to the AUC, a group classified as a terrorist organization, as either an ordinary business practice or as justified in pursuance of legitimate business interests.[144] Indeed, the court stressed that arms shipments for and payments to the AUC were not supplied "for ordinary commercial purposes, but were specifically intended to assist the AUC's military campaign against the FARC."[145] The purpose test was found to be met, even though the acts of the defendant corporation were

---

140. *Id.*

141. Presbyterian Church of Sudan v. Talisman Energy, Inc., 582 F.3d 244, 262 (2d Cir. 2009); Kiobel v. Royal Dutch Petroleum Co., 621 F.3d 111, 193 (2d Cir. 2010) (Leval, J., concurring in the judgment).

142. *Kiobel*, 621 F.3d at 158 (Leval, J., concurring in the judgment).

143. Doe I v. Nestle USA, Inc., 766 F.3d 1013, 1023–26 (9th Cir. 2014).

144. *Chiquita Brands Int'l*, 792 F. Supp. 2d at 1307, 1350–51.

145. *Id.* at 1350.

primarily motivated by its business interests.[146] Thus, where the activities go beyond the merely commercial or beyond the legitimate protection of a corporation's interests in the context of conducting business, a more relaxed version of purpose is instead applied. The definition of purpose was not confined to primary purpose and motive; the fact that the corporation was first and foremost motivated by financial interests did not exclude a secondary purpose of facilitating the violations carried out by the AUC, and the court was more easily prepared to infer the necessary purpose from the knowing actions of the corporation than in *Talisman* and *Kiobel.*

Sarei v. Rio Tinto demonstrates that the line that separates legitimate from illegitimate corporate activities is crossed where the corporation expressly demands that the government protect its business interests by carrying out gross human rights violations.[147] Such encouragement is considered to meet the standards of the purpose test.[148] This suggests a mixing of the actus reus and mens rea requirements, as encouragement is a particular form of aiding and abetting, not an element of mens rea.[149] Nevertheless, in the case of direct encouragement of the commission of human rights violations, it might be easier to infer a primary purpose that the corporation wants these violations to happen. This case also shows that the equation of motive and purpose can be misleading, as it is not clear that Rio Tinto acted with the primary purpose of bringing about human rights violations.[150] It is much more plausible that the corporation acted with the objective to maximize its profits and was prepared to pursue this goal through all necessary measures, including the direct encouragement of human rights violations. Comparing this with the case of Shell in *Kiobel,* where Shell allegedly discussed and supported a strategy to suppress the protest movement, knowing that violence would be used,[151] in both cases the corporation allegedly knew that the protection it wanted to obtain would involve the commission of gross human rights violations. The same can be said for the defendant in *Talisman.*[152] The main difference between the cases at the mens rea level seems to be that Talisman apparently would have preferred that the protection be provided without the human rights violations,[153] and that Shell might have hoped that its interests could be protected through legitimate means, even though both

146. *Id.* at 1348–49.

147. Sarei v. Rio Tinto, PLC, 671 F.3d 736, 766–67 (9th Cir. 2011) (en banc) (Schroeder, J., plurality opinion), *vacated*, 133 S. Ct. 1995 (2013).

148. *Id.*

149. *See, e.g.*, Prosecutor v. Furundžija, Case No. IT-95-17/1-T, Judgement, para. 235 (Int'l Crim. Trib. for the Former Yugoslavia Dec. 10, 1998) (finding that encouragement may satisfy the actus reus requirement).

150. The court found the plaintiffs' allegations sufficient to support a claim that Rio Tinto acted with intent to assist in the commission of war crimes. *See Rio Tinto*, 671 F.3d at 766–67 (Schroeder, J., plurality opinion) ("We conclude that the allegations are sufficient to state a war crimes claim."). Due to the Supreme Court's decision in *Kiobel*, however, it will never be known whether the plaintiffs could prove at trial that Rio Tinto's primary purpose was to cause the violations. *See* Sarei v. Rio Tinto, PLC, 722 F.3d 1109 (9th Circ. 2013) (mem.) (affirming dismissal of plaintiffs' claims on basis of sharp limitations as to applicability of ATS in *Kiobel*).

151. Kiobel v. Royal Dutch Petroleum Co., 621 F.3d 111, 189–90 (2d Cir. 2010) (Leval, J., concurring in the judgment).

152. Presbyterian Church of Sudan v. Talisman Energy, Inc., 582 F.3d 244, 262 (2d Cir. 2009).

153. *See id.* ("[P]laintiffs adduce evidence that senior Talisman officials protested to the Government and that security reports shared with senior Talisman officials expressed concern about the military's use of GNPOC airstrips.").

corporations knew that this was not going to happen.[154] Rio Tinto, on the other hand, requested the protection of its interests by the means of gross human rights violations.[155] This makes a difference not just regarding the mental element, but also at the actus reus level, as Rio Tinto's act went beyond indirect assistance and constituted active direct encouragement.[156]

All of this shows that the mens rea standard of purpose is not applied equally in all cases, but that it is employed in its strict version only where the act constituting the actus reus is regarded as a legitimate commercial act that results in indirect assistance to human rights violations, such as the building of all-weather roads as part of the infrastructure of an investment project. The nature of the act of assistance is thus relevant for the application of the purpose test in that courts are prepared to infer a purpose to assist in bringing about the violations where the act of providing assistance is either in itself unlawful or goes beyond a mere business activity, even if the primary aim was identified as making profit.

C. Concluding Remarks

As has become obvious, the various approaches to complicity liability under the ATS are highly influenced by the nature of the underlying act or transaction as commercial or business related. While the approaches differ dramatically, particularly with regard to the relevant mens rea standard, they are all driven by the shared conviction that the nature of the underlying act or transaction as commercial or business related provides it with a cloak of prima facie legitimacy that complicates the liability analysis significantly, particularly in the context of the provision of goods or services that might have legitimate as well as illegitimate uses. Before analyzing the different approaches, this Article will examine how comparable problems were addressed by courts in other contexts. These experiences will then inform the response to the main questions at the heart of this Article, i.e., how to draw the line between lawful and legitimate commercial transactions and corporate complicity.

II. COMPLICITY LIABILITY FOR DUAL-PURPOSE ACTS – LESSONS FROM THE AD HOC INTERNATIONAL CRIMINAL TRIBUNALS

Ad hoc international criminal tribunals, whose jurisprudence heavily influenced the liability standards applied by U.S. courts in corporate complicity cases under the ATS,[157] consistently apply an actus reus standard of an act of assistance that has a

154. *Kiobel*, 621 F.3d at 193 (Leval, J., concurring in the judgment); *Talisman*, 582 F.3d at 262.

155. *See Rio Tinto*, 671 F.3d at 766 (Schroeder, J., plurality opinion) (describing the defendant's request for "military action for its own private ends and directed the military response even 'while reports of war crimes surfaced'").

156. *See id.* ("These allegations support much more than 'an inference of mere knowledge on Rio Tinto's part; it supports an inference that Rio Tinto actively *encouraged* the killing of Bougainvilleans." (citation omitted)).

157. *See, e.g.*, Doe I v. Unocal Corp., 395 F.3d 932, 948 (9th Cir. 2002) (relying on standards set forth by the international criminal tribunals); *Kiobel*, 621 F.3d at 132–37 (stating that "the history and conduct of [international] tribunals is instructive" for deciding if corporations that allegedly aided and abetted the

substantial effect on the commission of the crime,[158] coupled with a mens rea test of knowledge, rather than purpose.[159] However, a recent controversy between different Appeals Chambers[160] shows that even outside the particular context of corporate complicity liability, courts struggle to apply these standards to aiding and abetting liability in cases of dual-purpose acts, i.e., where the act of assistance has the potential to contribute both to lawful and unlawful activities of the principal offender. This has clear similarities with the scenarios discussed in many of the corporate complicity cases under the ATS, such as the building of airstrips and all-weather roads in South Sudan.[161] While international criminal law does not provide for corporate liability,[162] it could well apply to the directors of corporations for aiding and abetting those crimes for which the ad hoc tribunals have jurisdiction.

The following discussion of two of the most recent decisions on aiding and abetting liability for dual purpose acts does not aim to assess the coherence of each approach in the context of the jurisprudence of the ad hoc international criminal tribunals and customary international law. Instead, it will limit itself to highlighting the reasons behind the different approaches to aiding and abetting liability and to assessing what can be learned from this for liability standards in the context of corporate complicity.

The Appeals Chamber of the International Criminal Tribunal for the Former Yugoslavia (ICTY) discussed the question of dual-purpose liability in *Perišić*.[163] Perišić was accused of having assisted in the commission of crimes carried out by the Army of the Republika Srpska (VRS) through various acts, including the large-scale

---

Nigerian government in committing human rights abuses were liable under the ATS).

158. Prosecutor v. Furundžija, Case No. IT-95-17/1-T, Judgement, para. 235 (Int'l Crim. Trib. for the Former Yugoslavia Dec. 10, 1998); Prosecutor v. Du[ko Tadi] (Prosecutor v. Tadić), Case No. IT-94-1-T, Judgment, para. 688 (Int'l Crim. Trib. for the Former Yugoslavia May 7, 1997); Prosecutor v. Blagojević, Case No. IT-02-60-A, Appeals Judgement, paras. 127, 134 (Int'l Crim. Trib. for the Former Yugoslavia May 9, 2007).

159. *See, e.g.*, *Furundžija*, Case No. IT-95-17/1-T, para. 245 (stating that "it is not necessary for the accomplice to share the *mens rea* of the perpetrator," but requiring only knowledge); Prosecutor v. Vasiljević, Case No. IT-98-32-A, Appeals Judgement, para. 102 (Int'l Crim. Trib. for the Former Yugoslavia Feb. 25, 2004) (requiring "knowledge that the acts performed by the aider and abettor assist the commission of the specific crime of the principal"); Prosecutor v. Aleksovski, Case No. IT-95-14/1-A, Appeals Judgement, paras. 162–63 (Int'l Crim. Trib. for the Former Yugoslavia Mar. 24, 2000) ("[I]t is not necessary to show that the aider and abettor shared the *mens rea* of the principal, but it must be shown that the aider and abettor was aware of the relevant *mens rea* on the part of the principal."); Prosecutor v. Perišić, Case No. IT-04-81-A, Appeals Judgement, para. 48 (Int'l Crim. Trib. for the Former Yugoslavia Feb. 28, 2013) (finding that the relevant requirement is "knowledge that assistance aids the commission of criminal acts, along with awareness of the essential elements of these crimes").

160. *Compare Perišić*, Case No. IT-04-81-A, para. 43 (reasoning in favor of an actus reus element of specific direction), *with* Prosecutor v. Šainović, Case No. IT-05-87-A, Appeals Judgement, para. 1649 (Int'l Crim. Trib. for the Former Yugoslavia Jan. 23, 2014) (deciding that specific direction "is not an element of aiding and abetting liability under customary international law"), *and* Prosecutor v. Taylor, Case No. SCSL-03-01-A, Appeals Judgment, para. 486 (Special Court for Sierra Leone Sept. 26, 2013) ("[T]he Appeals Chamber concludes that 'specific direction' is not an element of the actus reus of aiding and abetting liability . . . ."). As *Šainović* does not provide a discussion of issues relevant to this Article, the discussion will focus on the decisions in *Perišić* and *Taylor*.

161. Presbyterian Church of Sudan v. Talisman Energy, Inc., 582 F.3d 244, 249 (2d Cir. 2009).

162. *See* Ole Kristian Fauchald & Jo Stigen, *Corporate Responsibility Before International Institutions*, 40 GEO. WASH. INT'L L. REV. 1025, 1035–39 (observing that international law does not allow for corporate criminal liability).

163. *Perišić*, Case No. IT-04-81-A.

provision of military assistance, equipment, and supplies.[164] He, however, alleged that he had provided his assistance to support the (lawful) general war effort of the VRS, not to aid and abet the crimes it committed.[165] In *Perišić*, the Appeals Tribunal held that the actus reus of aiding and abetting liability not only required that the act have a substantial effect upon the perpetration of the crime, which is what most ICTY decisions limit their actus reus analysis to.[166] Rather, relying on the Appeals Chamber decision in *Tadić* which first defined the actus reus standard to be applied by the ICTY, *Perišić* held that it was also required that the act be "*specifically directed* to assist, encourage or lend moral support to the perpetration of a certain specific crime (murder, extermination, rape, torture, wanton destruction of civilian property, etc.)."[167]

According to the Appeals Chamber, the combination of substantial effect and knowledge alone could not in all cases adequately ensure that liability would only attach when a sufficient link between the accomplice and the principal offense exists, particularly where the accused is geographically removed from the commission of the offense, or the assistance consists of a dual-purpose act.[168] In such cases, the relevant link cannot be established simply by showing that the assistance made a substantial contribution to the crimes committed. Rather, in addition, "evidence establishing a direct link between the aid provided by an accused individual and the relevant crimes committed by principal perpetrators is necessary."[169]

The Appeals Chamber explained that specific direction "may involve considerations that are closely related to questions of *mens rea* [and] . . . evidence regarding an individual's state of mind may serve as circumstantial evidence that assistance he or she facilitated was specifically directed towards charged crimes."[170] This pragmatic approach aims to achieve at the actus reus level what the generally accepted test of knowledge prevents at the mens rea level; i.e., it aims to make liability subject to the requirement that the act be motivated by assisting an unlawful act.[171]

---

164. *Id.* paras. 2–3, 54.

165. *Id.* para. 20.

166. For an overview, see Prosecutor v. Šainović, Case No. IT-05-87-A, Appeals Judgement, paras. 1621–26 (Int'l Crim. Trib. for the Former Yugoslavia Jan. 23, 2014) (describing *Perišić* doctrine and subsequent applications).

167. *Perišić*, Case No. IT-04-81-A, para. 26 (citing Prosecutor v. Du[ko Tadi] (Prosecutor v. Tadić), Case No. IT-94-1-A, para. 229 (Int'l Crim. Trib. for the Former Yugoslavia May 7, 1997)).

168. *Id.* para. 39.

169. *Id.* para. 44.

170. *Id.* para. 48.

171. In favor of this approach, see *id.* para. 4 (Meron, J. and Agius, J., separate opinion); Kai Ambos & Ousman Njikam, *Charles Taylor's Criminal Responsibility*, 11 J. INT'L CRIM. JUST. 789, 804–07 (2013); Kevin Jon Heller, *Why the ICTY's "Specifically Directed" Requirement Is Justified*, OPINIO JURIS (June 2, 2013), http://opiniojuris.org/2013/06/02/why-the-ictys-specifically-directed-requirement-is-justified/. For a critical analysis see, for example Christopher Jenks, *Prosecutor v. Perišić. Case No. IT-04-81-A*, 107 AM. J. INT'L L. 622, 625 (2013); Marco Milanovic, *The Limits of Aiding and Abetting Liability: The ICTY Appeals Chamber Acquits Momcilo Perisic*, EJIL: TALK! (Mar. 11, 2013), https://www.ejiltalk.org/the-limits-of-aiding-and-abetting-liability-the-ICTY-appeals-chamber-acquits-momcilo-perisic/; James G. Stewart, *Guest Post: The ICTY Loses its Way on Complicity – Part 1*, OPINIO JURIS (Apr. 3, 2013) http://opiniojuris.org/2013/04/03/guest-post-the-icty-loses-its-way-on-complicity-part-1/ [hereinafter Stewart (2013(2))]. *See also Perišić*, Case No. IT-04-81-A, para. 3 (Liu, J., dissenting in part).

Addressing a question that has a clear parallel in the context of corporate complicity through commercial transactions with regimes that commit gross human rights violations, the Appeals Chamber emphasized that providing assistance to an organization that solely engages in criminal aims and activities might allow an inference that the assistance is specifically directed towards the commission of crimes.[172] General assistance to an organization that carries out legitimate as well as criminal activities, on the other hand, cannot automatically be construed as being specifically directed towards the furtherance of the criminal activities.[173] While evidence regarding the volume of assistance and knowledge of the crimes might establish substantial effect and "serve as circumstantial evidence of specific direction,"[174] it "does not automatically establish a sufficient link between aid provided by an accused aider and abettor and the commission of crimes by principal perpetrators."[175] Instead, specific direction is only established if it is "the sole reasonable inference after a review of the evidentiary record as a whole."[176]

Based on its understanding of the relevant legal principles, the Appeals Chamber held that specific direction could not be shown on any count of aiding and abetting of which Perišić was accused.[177] Even in light of the magnitude of the assistance provided, "the types of aid provided to the VRS do not appear incompatible with lawful military operations."[178] That the assistance was specifically directed "towards VRS crimes is [therefore] not the sole reasonable inference that can be drawn from the totality of the evidence on the record."[179] The overall conclusion was that

> while Perišić may have known of VRS crimes, the VJ aid he facilitated was directed towards the VRS's general war effort rather than VRS crimes. Accordingly, . . . Perišić was not proved beyond reasonable doubt to have facilitated assistance specifically directed towards the VRS Crimes in Sarajevo and Srebrenica.[180]

Applying this standard to corporate complicity cases, it would not be sufficient to show that a corporation knowingly provided substantial assistance for the commission of human rights violations. Instead, a direct link between the act of assistance and the violations would need to be established, for which it would not be sufficient to demonstrate the quantity and significance of the assistance. Rather, the only reasonable inference from all relevant facts would have to be that the assistance was specifically meant to further the human rights violations.[181] In the context of the

172. *Perišić*, Case No. IT-04-81-A, para. 48.

173. *Id.* paras. 52–53.

174. *Id.* paras. 56, 68.

175. *Id.* para. 56.

176. *Id.* para. 68.

177. *Id.*

178. *Perišić*, Case No. IT-04-81-A, para. 65.

179. *Id.* para. 57.

180. *Id.* para. 69.

181. *Id.* para. 56 (citing Prosecutor v. Krajišnik, Case No. IT-00-39-A, Appeals Judgement, para. 202 (Int'l Crim. Trib. for the Former Yugoslavia Mar. 17, 2009)); Prosecutor v. Stakić, Case No. IT-97-24-A, Appeals Judgement, para. 219 (Int'l Crim. Trib. for the Former Yugoslavia Mar. 22, 2006).

South Africa case,[182] for example, it would not be sufficient that financing was provided at a very large scale to the regime and its security forces, or that numerous military vehicles were sold to the regime. Liability would rather depend on whether it could be demonstrated that the money was loaned, or the vehicles sold, in order to assist the regime with carrying out its atrocious crimes and not to assist it with exercising its legitimate governmental tasks. However large scale the assistance, and notwithstanding the likelihood that the assistance would in reality go towards unlawful ends, no complicity liability would exist, unless it can be shown that it can only have been meant to further unlawful ends.

Just like the U.S. courts deciding cases of corporate complicity liability, the ICTY was primarily motivated by the wish to limit aiding and abetting liability to situations in which a sufficiently close link between the act of assistance and the crime can be established. However, the means through which the restriction is achieved differs from the various approaches under the ATS. It is not relevant that the act of assistance is inherently harmful. Nor is a direct purpose to bring about the violations required as part of the mens rea. However, in practice, the actus reus element of specific direction might be comparable to the purpose element of mens rea, as it requires that the assistance be specifically aimed at furthering the crimes committed, and knowledge alone is not sufficient to infer specific direction.

A few months after *Perišić*, the Appeals Chamber of the Special Court for Sierra Leone (SCSL) disagreed with *Perišić* in its *Taylor* decision on the crucial point of whether specific direction is necessary to establish a sufficiently close link between the accomplice and the crime, particularly in cases of dual purpose assistance.[183] The Appeals Chamber of the SCSL insisted that this role could satisfactorily be assumed by the actus reus element of substantial effect[184] and that a case-by-case analysis of the necessary proximity of the accomplice to the crime was both necessary and sufficient to distinguish the culpable from the innocent.[185] Specifying further the criteria that should inform the actus reus analysis in each case, the Appeals Chamber suggested that:

> Merely providing the means to commit a crime is not sufficient to establish that an accused's conduct was criminal. Where the crime is an isolated act, the very fungibility of the means may establish that the accused is not sufficiently connected to the commission of the crime. Similarly, on the facts of a case, an accused's contribution to the causal stream leading to the commission of the crime may be insignificant or insubstantial, precluding a finding that his acts and conduct had a substantial effect on the crimes. In terms of the effect of an accused's acts and conduct on the commission of the crime through his assistance to a group or organisation, there is a readily apparent difference between an isolated crime and a crime committed in furtherance of a widespread and systematic attack on

182. *In re* S. African Apartheid Litig., 617 F. Supp. 2d 228 (S.D.N.Y. 2009).

183. Prosecutor v. Taylor, Case No. SCSL-03-01-A, Appeals Judgment, paras. 473–80 (Special Court for Sierra Leone Sept. 26, 2013).

184. *Id.* para. 390.

185. *Id.* paras. 390–92, 480.

> the civilian population. The jurisprudence provides further guidance, but it is the differences between the facts of given cases that are decisive.[186]

The Appeals Chamber thus embraces a case-by-case approach to the substantiality of the act of assistance. Of particular relevance for the discussion of corporate complicity liability is the suggestion that the focus of the liability analysis needs to be on the actual effect of the assistance on the crime, not on its potential effect based on the nature of the product or service provided.[187] This differs considerably from the approach to the actus reus element adopted in In re *South African Apartheid Litigation*.[188]

Taylor also highlighted the importance of the qualitative and not just quantitative effect of assistance, e.g., where the accomplice, as in the case of Charles Taylor, provides supplies at a particularly crucial time.[189] It further stressed that "an accused need not be the only source of assistance in order for his acts and conduct to have a substantial effect on the commission of the crimes."[190] Therefore, that only some of the supplies used for the commission of a crime can be attributed to the accomplice does not exclude liability but rather requires a thorough analysis of whether, taking into consideration the other sources of assistance, the accomplice's "acts and conduct had a substantial effect on the commission of the crimes."[191]

Even though Charles Taylor was physically remote from the crimes committed, the Appeals Chamber confirmed his conviction as an accomplice because of the extensive, sustained, and vital nature of the assistance, and the key impact it had on the commission of the crimes.[192] Moreover, "in addition to knowing of the [Revolutionary United Front (RUF)]/[Armed Forces Revolutionary Council (AFRC)]'s intent to commit crimes, Taylor was aware of the specific range of crimes being committed during the implementation of the RUF/AFRC's Operational Strategy and was aware of the essential elements of the crimes."[193] He consequently also acted with the relevant mens rea.[194]

The decision in *Taylor* shows that it is possible to determine the link between the assistance and the offense committed that is necessary to justify imposing aiding and abetting liability by combining an actus reus standard of substantial effect—to be established on a case-by-case basis—with a mens rea standard of knowledge. In providing some interesting reflections on the elements that guide a case-by-case determination of substantial effect, many of which could equally be relevant for the actus reus assessment in corporate complicity cases, it offers an interesting alternative to the approach adopted in In re *South African Apartheid Litigation*.

The *Taylor* decision has drawn criticism, though, in particular because of its "reliance on a vague 'substantial effect' requirement as the lone physical limitation

---

186. *Id.* para. 391.

187. *Id.* para. 394.

188. *In re* S. African Apartheid Litig., 617 F. Supp. 2d 228, 264–65 (S.D.N.Y. 2009) (placing importance on the nature of the product provided).

189. *Taylor*, Case No. SCSL-03-01-A, para. 514.

190. *Id.* para. 516.

191. *Id.*

192. *Id.* para. 520.

193. *Id.* para. 540.

194. *Id.*

on complicity liability"[195] and for leaving "undefined the distinction between innocent and culpable aid in cases where," unlike in *Taylor* itself, "the provision of assistance is not essential to the commission of an underlying offense."[196] This criticism is largely based on concerns specific to the context of international criminal law, which requires clarity in order not to lose legitimacy, and because individual criminal liability requires a high degree of legal certainty and foreseeability.[197]

In light of *Taylor*, an analysis of the actus reus of corporate complicity liability would require a thorough examination of all the factors of the individual case. Where, for example, money is provided to a regime that commits gross human rights violations, liability would depend on how substantially the money assisted in the violations carried out by the regime, in light of all the different income sources it had at its disposal. Similarly, regarding the sale of military vehicles, liability would depend on the systematic nature of the violations carried out with their help and how important the vehicles provided were for the commission of the offenses, among other factors. At the same time, given that no showing of direct assistance is necessary,[198] no link between the actual good sold and the violation carried out would need to be established. Thus, a defendant could not avoid liability by alleging that massacres carried out could not be linked to the precise vehicle sold, or the money lent.

The dispute between the two Appeals Chambers in *Perišić* and *Taylor*[199] closely reflects the debate of the feasible liability standard in the context of corporate complicity, in particular regarding whether a combination of substantial effect at the objective level, and knowledge at the subjective level, leads to boundless liability or whether, if taken seriously, these criteria together can strike an adequate balance between overinclusiveness and impunity. Just like in the context of corporate complicity under the ATS, the choice of liability standard seems to have depended largely on whether it was regarded to be unacceptable to provide knowing assistance only if it is clearly meant exclusively to be used for unlawful purposes, or whether assistance that has a dual purpose should result in liability if it is made with the knowledge that it will substantially further unlawful purposes.

III. U.S. DOMESTIC CRIMINAL COMPLICITY CASES IN THE CONTEXT OF COMMERCIAL TRANSACTIONS

Important insights for the question of how to draw the line between legitimate business transactions and acts that trigger complicity liability can also be gained from

195. Recent Case, *Special Court for Sierra Leone Rejects "Specific Direction" Requirement for Aiding and Abetting Violations of International Law*—Prosecutor v. Taylor, 127 HARV. L. REV. 1847, 1851 (2014).

196. *Id.*

197. *Id.* at 1851, 1853–54.

198. *Taylor*, Case No. SCSL-03-01-A, paras. 357, 362.

199. The decision in *Prosecutor v. Šainović*, Case No. IT-05-87-A, Appeals Judgement (Int'l Crim. Trib. for the Former Yugoslavia Jan. 23, 2014), in which the Appeals Chamber of the ICTY held, in clear disagreement with *Perišić*, that the actus reus of aiding and abetting liability does not require a demonstration of specific direction, has not been discussed because the decision does not provide a detailed discussion of the implications of applying or rejecting a specific direction requirement on the facts of the case, but rather focuses its analysis on the legal question of the relevant standard. *Id.* paras. 1617–51.

U.S. domestic complicity cases. Quite a few courts had to tackle the problem of the limits of complicity liability, in the form of conspiracy, aiding and abetting, or both, where the act of assistance consisted of a commercial transaction.

In U.S. criminal law, it seems that, in principle, every act of assistance can qualify for aiding and abetting liability, without any requirement that it have a substantial effect on the commission of the crime.[200] This, of course, would potentially lead to very far-reaching liability, particularly in the commercial context, which might explain why courts put a lot of effort into finding principles according to which such liability can be limited.

A good starting point for an analysis of criminal complicity cases is provided by the influential *Peoni* case, which introduced a mens rea test of purpose to U.S. criminal complicity law. In *Peoni*, Judge Learned Hand made the often repeated statement that the various definitions of complicity liability "have nothing whatever to do with the probability that the forbidden result would follow upon the accessory's conduct."[201] Instead, "they all demand that he in some sort associate himself with the venture, that he participate in it as in something that he wishes to bring about, that he seek by his action to make it succeed. All the words used—even the most colorless, 'abet'—carry an implication of purposive attitude towards it."[202] This very closely resembles the purpose test applied by many courts in the context of ATS litigation and makes clear that mere knowledge, coupled with a relevant act of assistance, would not suffice to trigger complicity liability.

Of particular relevance for corporate complicity liability is *Falcone*, a case where the complicity charge was based on the accusation that the defendant had sold large amounts of sugar, i.e., a product that clearly has lawful uses and no inherently harmful qualities (at least none that are relevant in the context of the commission of crime) to customers who then sold it to illegal distilleries.[203] The question before the court was "whether the seller of goods, in themselves innocent, becomes . . . an abettor of . . . the buyer because he knows that the buyer means to use the goods to commit a crime."[204] The court issued a strong warning against an approach that attributes liability simply because someone "does not forego a normally lawful activity, of the fruits of which he knows that others will make an unlawful use."[205] Such a doctrine would carry a risk "of great oppression"[206] which can only be avoided by closely limiting the scope of liability to the cases in which the accomplice "in some sense promote[s] their venture himself, make[s] it his own, ha[s] a stake in its outcome."[207]

Falcone was sometimes relied on for the suggestion that legal sales can never amount to conspiracy, even if the seller knows that they will be used for illegal

200. 18 U.S.C. § 2(a) (2014); Baruch Weiss, *What Were They Thinking?: The Mental States of the Aider and Abettor and the Causer Under Federal Law*, 70 FORDHAM L. REV. 1341, 1347–48 (2002).

201. United States v. Peoni, 100 F.2d 401, 402 (2d Cir. 1938).

202. *Id.*

203. United States v. Falcone, 109 F.2d 579, 580 (2d Cir. 1940) (describing how plaintiff sold large quantities of sugar to grocers who subsequently sold the sugar to illegal distilleries).

204. *Id.* at 581.

205. *Id.*

206. *Id.*

207. *Id.*

purposes.[208] However, this view was rejected by the U.S. Supreme Court in *Direct Sales*.[209] A registered drug manufacturer and wholesaler who conducted a nationwide mail-order business had supplied a registered physician with vast quantities of morphine sulphate, which the latter then illegally distributed to addicts.[210] The Court held that *Falcone* does not stand for a general proposition that "one who sells to another with knowledge that the buyer will use the article for an illegal purpose cannot, under any circumstances, be found guilty of conspiracy with the buyer to further his illegal end."[211] Liability would instead depend on the nature of the commodities sold. While the goods in *Falcone* were sugar, cans, and other such goods, and therefore articles of free commerce, the morphine sulphate sold in *Direct Sales* was a restricted commodity, "incapable of further legal use except by compliance with rigid regulations."[212] The significance of this difference was

> like that between toy pistols or hunting rifles and machine guns. All articles of commerce may be put to illegal ends. But all do not have inherently the same susceptibility to harmful and illegal use. Nor, by the same token, do all embody the same capacity, from their very nature, for giving the seller notice the buyer will use them unlawfully. Gangsters, not hunters or small boys, comprise the normal private market for machine guns. So drug addicts furnish the normal outlet for morphine which gets outside the restricted channels of legitimate trade.[213]

For the Court, the relevance of the nature of the goods was twofold: to make "certain that the seller knows the buyer's intended illegal use . . . [and] to show that by the sale he intends to further, promote and cooperate in it."[214] Regarding the relationship between intent and knowledge, the Court observed that even though intent "is not identical with mere knowledge that another purposes unlawful action, it is not unrelated to such knowledge. Without the knowledge, the intent cannot exist."[215] Whether goods have an inherent capacity for harm or have their sale restricted "makes a difference in the quantity of proof required to show knowledge that the buyer will utilize the article unlawfully."[216] However, "not every instance of sale of restricted goods, harmful as are opiates, in which the seller knows the buyer intends to use them unlawfully, will support a charge of conspiracy."[217] This would rather depend on additional facts, such as whether a single transaction rather than a

---

208. *See* United States v. Piampiano, 271 F.2d 273, 274 (2d Cir. 1959) (noting appellant's reliance on *Falcone* for the proposition that "a mere supplier, even one aware of the illegal purpose of his purchaser, cannot be held as a co-conspirator").

209. *See* Direct Sales Co. v. United States, 319 U.S. 703, 714–15 (1943) (holding that a registered drug manufacturer participated in a conspiracy to illegally distribute drugs when he frequently sold a physician large quantities of morphine sulphate by mail with the intent to further the physician's illegal drug sales, even though the sales were facially lawful).

210. *Id.* at 704–05.

211. *Id.* at 709.

212. *Id.* at 710.

213. *Id.*

214. *Id.* at 711.

215. *Direct Sales*, 319 U.S. at 711.

216. *Id.*

217. *Id.* at 712.

continuous business relationship was at issue, and whether it involved "nothing more on the seller's part than indifference to the buyer's illegal purpose and passive acquiescence in his desire to purchase."[218]

The Court concluded from the aggressive sales practices of the supplier of the morphine sulphate and the long cooperation with the physician who supplied this drug illegally to addicts that the defendant not only knew and acquiesced, but moreover had "a 'stake in the venture' which, even if it may not be essential, is not irrelevant to the question of conspiracy,"[219] the stake being "making the profits which it knew could come only from its encouragement of Tate's illicit operations."[220]

Liability thus followed from a combination of different factors, ranging from the nature of the goods as restricted so that they could not be sold on the free market, to the sales practices and the duration of the buyer/seller relationship. In addition to knowledge, intent was necessary which could not be inferred from knowledge alone, but from knowledge coupled with particular features of the act of assistance, such as its continuous nature.[221] The nature and intensity of the act of assistance is thus relevant primarily for an inference of the mens rea in the form of knowledge and intent, but is not regarded as fulfilling the function of weeding out, already at the actus reus level, acts that simply are not sufficiently pertinent to qualify as criminally relevant assistance with the principal offense. It is not clear, on the other hand, what level of knowledge would be required to infer intent where the goods at issue were neutral and/or unrestricted.

For corporate complicity liability, this would have the implication that liability might, just like the court in In re *South African Apartheid Litigation* suggested,[222] be highly influenced by the nature of the goods and services as harmless, neutral or unrestricted, as opposed to inherently harmful or restricted by law. However, the impact of this does not materialize at the actus reus level. Instead it influences the quantity of proof required to establish knowledge of and intent regarding the unlawful use that will be made of the goods provided, which can be inferred much more easily where the nature of the good invites such a use. However, even in the case of restricted or inherently harmful goods, a case-by-case analysis is necessary to determine the actual existence or absence of knowledge and intent. Given that intent requires having a stake in the venture,[223] corporate complicity liability would then depend on questions such as whether the corporation benefits from the successful commission of the principal offense. While this might exceptionally be the case in situations such as that of *Rio Tinto*,[224] in most cases of corporate complicity in human rights violations it will be difficult to satisfy this criterion. For example, in In

218. *Id.* at 712 n.8.

219. *Id.* at 713.

220. *Id.*

221. *See Direct Sales*, 319 U.S. at 711, 713 (stating that "[w]hile [intent] is not identical with mere knowledge that another purposes unlawful action, it is not unrelated to such knowledge," and when there is "prolonged cooperation" there is "no legal obstacle to finding that [the party] not only knows and acquiesces, but joins both mind and hand" with the principal to commit the crime).

222. *In re* S. African Apartheid Litig., 617 F. Supp. 2d 228, 258–59 (S.D.N.Y. 2009).

223. *See Direct Sales*, 319 U.S. at 713 (finding allegations were sufficient to support theory of liability because defendant had acquired a stake in the venture).

224. Sarei v. Rio Tinto, PLC, 671 F.3d 736, 766 (9th Cir. 2011) (Schroeder, J., plurality opinion) (discussing allegations that Rio Tinto solicited war crimes to protect its economic interests), *vacated*, 133 S. Ct. 1995 (2013).

re *South African Apartheid Litigation*, for the corporations' business interests it will have been irrelevant whether or not the military committed extrajudicial killings with the vehicles sold.[225] This might be different in cases where sales of particular goods soar because of the human rights violations for which they are needed, for example where the demand for weapons depends on sustaining the conflict or repression in a given country, or where goods are specifically tailored for the commission of violations, such as the computer programs that were designed to implement apartheid policies.

In light of *Falcone* and *Direct Sales*, some courts answered the question that the court in *Blankenship* aptly summarized as "Where does the 'mere' sale end, the conspiracy begin?"[226] by stating that the supply of "goods, innocent in themselves . . . to a purchaser who, to the supplier's knowledge, intends to and does use them in the furtherance of an illegal conspiracy"[227] does not cross the complicity threshold.[228] In *Blankenship*, however, a case in which one of the defendants leased his house trailer to a group that was to use it to cook methamphetamine, accepted a down-payment for the lease but then got cold feet and dropped out of the agreement,[229] the court was not entirely convinced by the approach adopted in those two cases. While "[o]ne may draw a line, as *Falcone* and *Direct Sales* did, between knowledge of other persons' crimes and intent to join them,"[230] the court expressed doubts that the criteria to determine the circumstances in which an inference of intent to join was permissible were delineated clearly enough by the courts.[231] It suggested instead that a more functional approach would be to ask "whether the imposition of liability on transactions of the class depicted by the case would deter crime without adding unduly to the costs of legitimate transactions."[232] Thus, the court moved the focus of the analysis from the mens rea of wishing the crime to succeed to policy considerations of deterrence and a cost/benefit assessment of imposing liability.

This modified approach built on several decisions in which courts applied a mens rea test of purpose but centered the liability analysis on the deterrence of crime. The question of deterrence lay, for example, at the heart of the discussions of hypothetical complicity scenarios related to prostitution, presented in slight variation in different decisions. *Fountain*, for example compared two hypothetical cases:

> In the first, a shopkeeper sells dresses to a woman whom he knows to be a prostitute. The shopkeeper would not be guilty of aiding and abetting prostitution unless the prosecution could establish the elements of Judge

225. *See* In re *S. African Apartheid Litig.*, 617 F. Supp. 2d at 243 (discussing the sale of military vehicles to the South African government).

226. United States v. Blankenship, 970 F.2d 283, 286 (7th Cir. 1992).

227. United States v. Campisi, 306 F.2d 308, 310 (2d Cir. 1962) (quoting United States v. Tramaglino, 197 F.2d 928, 930 (2d Cir. 1952)).

228. *Id.* at 310–11.

229. *Blankenship*, 970 F.2d at 284.

230. *Id.* at 286.

231. *See id.* (arguing that differentiating between a mere sale of goods and participation in a conspiracy by drawing a line between knowledge of other persons' crimes and intent to join them is problematic because it restates the elements of a conspiracy without indicating "when an inference of intent to join is permissible").

232. *Id.* at 287.

> Hand's test. Little would be gained by imposing criminal liability in such a case. Prostitution, anyway a minor crime, would be but trivially deterred, since the prostitute could easily get her clothes from a shopkeeper ignorant of her occupation. In the second case, a man buys a gun from a gun dealer after telling the dealer that he wants it in order to kill his mother-in-law, and he does kill her. The dealer would be guilty of aiding and abetting the murder. This liability would help to deter—and perhaps not trivially given public regulation of the sale of guns—a most serious crime. We hold that aiding and abetting murder is established by proof beyond a reasonable doubt that the supplier of the murder weapon knew the purpose for which it would be used.[233]

Thus, deterrence considerations made the court move from a standard of purpose to one of knowledge if commercial transactions assist with the commission of the most serious crimes: "One who sells a gun to another knowing that he is buying it to commit a murder, would hardly escape conviction as an accessory to the murder by showing that he received full price for the gun."[234] The fact that the act of assistance will in all likelihood have been primarily, if not exclusively, motivated by business considerations is clearly regarded to be irrelevant in this scenario. Under this approach, a mens rea test of knowledge should be sufficient in corporate complicity cases, given the seriousness of the human rights violations that are at stake in these cases.

In *Giovannetti*, the court further developed the policy considerations raised in *Fountain*, and approached the question of triviality slightly differently. Changing the example to the sale of an address book to a prostitute, the court observed that the seller

> can hardly be said to be seeking by his action to make her venture succeed, since the transaction has very little to do with that success and his livelihood will not be affected appreciably by whether her venture succeeds or fails. And, what may well be the same point seen from another angle, punishing him would not reduce the amount of prostitution—the prostitute, at an infinitesimal cost in added inconvenience, would simply shop for address books among stationers who did not know her trade.[235]

The observation that deterrence would not be served by punishing the seller of the address book, as it could easily be obtained elsewhere from an unsuspecting seller, is interesting and goes back to the question of the free availability of the goods on the market, raised by the Supreme Court in *Direct Sales*.[236] However, decreasing crime generally is not the only goal of deterrence. At the individual level, deterrence aims to discourage individuals from committing criminal acts with the relevant mens rea.[237] To exclude an act from any form of liability on the basis that someone else

233. United States v. Fountain, 768 F.2d 790, 798 (7th Cir. 1985).

234. *Id.* (quoting Backun v. United States, 112 F.2d 635, 637 (4th Cir. 1940))

235. United States v. Giovanetti, 919 F.2d 1223, 1227 (7th Cir. 1990).

236. *See* Direct Sales Co. v. United States, 319 U.S. 703, 710 (1943) (discussing the relevance to the analysis of "articles of free commerce," such as toy pistols).

237. Weiss, *supra* note 200, at 1484.

would have done the same, with or without the relevant mens rea, completely ignores the individual aspect of deterrence and would result in unjustified impunity of those who themselves meet the applicable liability criteria. The relevant question should therefore not be whether the assistance would have easily been available from other sources, but rather whether or not the act of assistance, if carried out with the relevant mens rea, was substantial enough for the commission of the crime to warrant the accomplices criminal liability.

If, as *Giovannetti* suggests, it was decisive whether the seller's livelihood depended on the success of the principal offense, this would presumably also exclude the liability of the seller of the gun in the *Fountain* example, for it can hardly be relevant to the seller whether or not the buyer commits murder with the gun, uses it for lawful purposes, or does not use it at all. More relevant seems to be the court's statement that "the transaction has very little to do" with the success of the crime,[238] which points towards the requirement of a link between the assistance rendered and the principal offense. In all of these cases this issue was regarded as a mens rea consideration. Only where a sufficient link exists between the assistance and the crime can it be inferred that by rendering the assistance the accomplice desired its success.

Blankenship brought yet another consideration into the discussion of the prostitution examples. The court commented that to hold the stationer in the prostitution example liable as an accomplice would not significantly deter prostitution, but "raise the costs of legitimate business, for it would either turn sellers into snoops (lest they sell to the wrong customers) or lead them to hire blind clerks (lest they learn too much about their customers); either way, the costs of business would rise, and honest customers would pay more."[239] It is not, however, clear why complicity liability would create the risk of turning businesspeople into snoops and thereby raise the costs of legitimate business transactions, as none of the liability standards under discussion in the criminal law context impose on businesses the obligation to find out the motivations behind the commercial transactions of their customers. As the court in *Blankenship* itself explains, "[b]ecause a lessor almost inevitably knows his tenant's business, the imposition of a criminal penalty is likely to deter but not to raise the costs of legitimate transactions."[240] If liability depends on actual knowledge, which seems to be the minimum mens rea standard in criminal complicity cases, the imposition of liability would not raise the costs of legitimate transactions while potentially deterring those that further crime.

In *Irwin*, though not in the context of assistance in the form of commercial transactions, the court provided an interesting analysis of the interrelatedness of the various elements of complicity liability. The court highlighted that in cases "where the evidence of the defendant's intent must be inferred from the aid given,"[241] the act and intent elements of complicity liability "really merge and our review focuses on whether the aid given was sufficient to support the inference of intent to further the crime."[242] The court suggested that "[b]ecause the aid that the defendant gave often

238. *Giovanetti*, 919 F.2d at 1227.

239. United States v. Blankenship, 970 F.2d 283, 287 (7th Cir. 1992).

240. *Id.*

241. United States v. Irwin, 149 F.3d 565, 572 (7th Cir. 1998).

242. *Id.*

pulls double duty . . . as direct evidence of affirmative assistance and circumstantial evidence of intent,"[243] a case might be made to modify the analysis by focusing instead "on the amount of assistance knowingly given."[244] It then discussed in some detail the implications of removing any requirement for desire to make the offense succeed from the mens rea of complicity liability and commented that it was unlikely that someone would provide material assistance without any desire that the crime succeed.[245] Instead, "[m]aterial assistance deliberately given is *itself* evidence of intent."[246] This differs fundamentally from *Peoni* and *Falcone,* as it can hardly be said that every accomplice who provides deliberate assistance has a stake in the venture.

The court in *Irwin* was reluctant to drop the intent element completely and rather suggested that liability would be justified either where material assistance was rendered knowingly, or where minor assistance was provided with intent.[247] Regarding the threshold the act of assistance must meet to justify an inference of intent, the court ruled out that trivial assistance could support such an inference, while critical assistance clearly would,[248] and emphasized that "[t]here is no magic formula to easily determine on which side of the sufficiency line the evidence in a case falls."[249] Thus, a case-by-case analysis would be necessary to determine whether, in any given case, the assistance was sufficiently important to justify an inference of intent.

The analysis of these cases shows that in domestic criminal law cases, U.S. courts apply a mixture of approaches in order to limit complicity liability for commercial acts that assist with the commission of criminal offenses. Even though, in principle, any act of assistance seems to be sufficient to satisfy the actus reus requirement of complicity liability, without having to meet a substantiality or materiality threshold, courts generally agree that the application of such a test would lead to too far-reaching liability in the context of commercial transactions. Since the influential *Peoni* decision, most courts seem to have accepted that intent in these cases cannot simply be inferred from knowing participation, but instead requires a showing that the accomplice have a stake in the venture. This, however, has caused its own problems, which courts try to overcome in different ways. Some courts shift the focus of the analysis to questions of deterrence and the costs of imposing liability on ordinary commercial activities;[250] others consider the impact of the substantial or trivial nature of the goods and the transactions on inferring both knowledge and intent.[251] The seriousness of the principal offense is another consideration.[252]

---

243. *Id.*

244. *Id.*

245. *Id.*

246. *Id.*

247. *Irwin*, 149 F.3d at 572–73

248. *Id.* at 573.

249. *Id.*

250. United States v. Blankenship, 970 F.2d 283, 287 (7th Cir. 1992).

251. *See* Direct Sales Co. v. United States, 319 U.S. 703, 710–15 (1943) (relying on distinctions between restricted goods that are inherently susceptible to harmful or illegal use and "normal goods" and the distinction between isolated, small-scale sales and recurring large-scale sales to find that suppliers engaging in massive sales of goods that are inherently susceptible to illegal use likely acted with intent).

252. *See* United States v. Fountain, 768 F.2d 790, 798 (7th Cir. 1985) (suggesting that courts may take into account the seriousness of the offense when determining whether a supplier is criminally liable for aiding and abetting).

IV. ASSESSING THE DIFFERENT LIABILITY STANDARDS

The preceding overview of case law from different contexts shows that the attribution of secondary liability in the context of acts that are facially lawful or could serve both lawful and unlawful purposes is complex and highly controversial. The one clear tendency that all approaches share is that of searching for criteria according to which to limit liability to cases where a sufficient link between the assistance and the principal offense can be established. Fundamental differences, however, materialize when it comes to the question of what link to regard as necessary and sufficient to justify the imposition of complicity liability in the context of commercial transactions. The answer to this question seems to depend largely on each court's view of how the various interests and policy considerations should be balanced, and, in particular, under what circumstances an otherwise legitimate act turns into an unlawful act of assistance in a third party's crimes or human rights violations.

As has become obvious, the various approaches to complicity liability under the ATS and U.S. domestic criminal law are highly influenced by the nature of the underlying act or transaction as commercial or business related. However, unless commercial acts are per se exempt from complicity liability, which is not an approach favored by any of the courts dealing with corporate complicity cases, to identify the underlying act as commercial can and should be only the starting point of the discussion, focusing the analysis on whether this nature of the act justifies specific liability standards, and if so, which.

While agreement exists that carrying out ordinary business transactions or other lawful acts with the knowledge that they might assist in gross human rights violations or crimes, without more, should not give rise to liability, differences arise with regard to what more is required to justify the imposition of aiding and abetting liability. This question has been answered differently by different courts. One approach combines an actus reus test of substantial effect with a mens rea requirement of knowledge. Within that approach, differences exist as to whether the question of substantial effect should be determined on a case-by-case basis,[253] by adopting an approach that focuses on the nature of the assistance,[254] or by requiring that the act be specifically directed to the commission of unlawful acts.[255]

Closely linked to the approach in *Perišić*, other courts restrict liability primarily at the mens rea level and require a mens rea of primary purpose[256] or intent in the form of having a stake in the success of the principal offense.[257] The focus in *Doe I v. Nestle* on the fact that the defendant corporations directly benefited from the human

253. Prosecutor v. Taylor, Case No. SCSL-03-01-A, Appeals Judgment, paras. 368–70 (Special Court for Sierra Leone Sept. 26, 2013).

254. *In re* S. African Apartheid Litig., 617 F. Supp. 2d 228, 258–59 (S.D.N.Y. 2009).

255. Prosecutor v. Perišić, Case No. IT-04-81-A, Appeals Judgement, para. 36 (Int'l Crim. Trib. for the Former Yugoslavia Feb. 28, 2013).

256. Presbyterian Church of Sudan v. Talisman Energy, Inc., 582 F.3d 244, 258–59 (2d Cir. 2009).

257. United States v. Falcone, 109 F.2d 579, 581 (2d Cir. 1940); United States v. Peoni, 100 F.2d 401, 402 (2d Cir. 1938).

rights violations[258] points in a similar direction. Other courts to some extent combine the evaluation of actus reus and mens rea elements and make the evidence that is necessary to infer knowledge and intent at the mens rea level dependent on the nature of the act.[259]

It becomes clear that the commercial nature of the act of assistance has an impact on approaches both to the actus reus and mens rea in complicity cases. Given that the liability standards, at the actus reus and mens rea levels (and combined), play the role of determining the "more" that is necessary to turn a commercial activity into an act of corporate complicity, it is important to be clear about the implications of the different approaches that can be adopted in this respect. If the "more" is to be found at the actus reus level, it would have to embody an activity that goes beyond making a mere commercial transaction. In a mens rea–based interpretation, on the other hand, the "more" would be the mental element with which the commercial transaction was carried out. Where both elements are combined, it might well be that stricter actus reus standards can be balanced out by relaxing the mens rea standard or vice-versa.

A. The Actus Reus Analysis

In the context of commercial transactions, no courts seem to adopt the approach that the knowing provision of any assistance, however trivial, results in complicity liability. Instead, all courts that apply a knowledge standard of mens rea require some form of materiality or substantiality of the act of assistance for the commission of the principal offense. Indeed, the triviality of the assistance in the prostitution examples given by U.S. courts in the domestic criminal complicity context makes clear why assistance that has no more than a minimal effect on the commission of the offense should not result in liability.

However, in the context of commercial transactions, particularly the provision of goods or services that might have legitimate as well as illegitimate uses, to determine the materiality or substantial effect of assistance can be difficult.[260] This is because in many cases no direct link between the assistance and the violations can easily be established, for example where fungible goods are provided by several corporations to a regime that might use them for lawful as well as unlawful purposes. It will then often be impossible to determine whose goods were used for violations and whose for lawful purposes. To determine with precision at which point assistance crosses the threshold from the trivial to the substantial also might not always be obvious.

The court in In re *South African Apartheid Litigation* tried to overcome these difficulties by making the decision of whether or not assistance has a substantial effect on the commission of human rights violations dependent on objective characteristics of the act of assistance.[261] In cases in which the act of assistance

258. Doe I v. Nestle USA, Inc., 766 F.3d 1013, 1024 (9th Cir. 2014).

259. Direct Sales Co. v. United States, 319 U.S. 703, 711–12 (1943).

260. It has even been argued in this context that this "intermix of both socially injurious and neutral uses frustrates any fair and rationale, [sic] let alone evidentiary [sic] feasible, imputation of consequences to remotely involved business actors who contributed to the causal chain of events long before the actual commission of a core crime." Burchard, *supra* note 57, at 938.

261. *In re* S. African Apartheid Litig., 617 F. Supp. 2d 228, 257–58 (S.D.N.Y. 2009).

consists of the lawful provision of commercial goods or services that do not have inherently harmful qualities and are not the direct means through which the violations are carried out, the actus reus of aiding and abetting liability is not met, so that such acts are exempt from complicity liability.[262] While this question was not expressly addressed by the court, this would presumably apply even if such an act was motivated by the purpose of bringing about gross human rights violations. However, a business activity can no longer be regarded as neutral and exempt from liability if it consists of providing the direct means through which a violation is carried out, if the goods or services provided are inherently harmful, or where goods or services are specifically tailored to assisting the business partner with the violations.[263] Such acts, combined with knowledge that the activities have a substantial effect on the commission of the violations, pass the complicity threshold.[264]

To limit the actus reus in cases of commercial activities in such an absolute way might have the advantage of providing a clear-cut approach which removes the need to develop more refined criteria according to which the substantial effect of commercial activities on gross human rights violations can be established.[265] However, while it is necessary to find a principled way to distinguish between acceptable business activities and those that give rise to complicity liability, and to avoid casting the net so widely that corporations are held indiscriminately liable for all offenses committed by regimes with which they do business, the approach to the actus reus of aiding and abetting liability adopted in In re *South African Apartheid Litigation* raises several fundamental problems.[266]

In eliminating any need to perform a case-by-case analysis of the effect of the act of assistance on the violation, and of the closeness of the defendant to it, this approach shields certain acts (such as the sale of goods that are not inherently harmful but might potentially be used for harmful purposes) automatically from liability. A corporation could, for example, escape liability by selling only commercial, but not military, vehicles to a regime, with the knowledge or even intent that they will be used to commit gross human rights violations. At the same time, it seems that the inherently harmful nature of the goods or services in and of itself gives rise to an assumption of substantial effect, whether or not this effect actually materializes in the individual case.[267] This is an anomaly in both criminal and civil

262. *Id.*

263. *Id.* at 257–59.

264. *Id.* at 257–59, 262.

265. Indeed, this approach seems to have motivated the South African government to change its mind. After the actus reus standard had been limited in this way, it withdrew its objection to the apartheid litigation in the United States. Jeff Radebe, South Africa's Minister of Justice, commented that because the court dismissed the claims that were considered to be based solely on the fact that the defendant corporation had been doing business with the apartheid regime, and upheld only those claims that referred to corporate aiding and abetting in the commission of serious crimes under international law, its concerns no longer persisted. Letter from Jeffrey Radebe, Minister of Justice and Constitutional Dev., Republic of S. Afr., to Shira A. Scheindlin, Judge, U.S. Dist. Court for the S. Dist. of N.Y. (undated), *available at* http://www.khulumani.net/khulumani/documents/file/12-min.justice-jeff-radebe-letter-to-us-court-2009.html.

266. For an in-depth discussion, see generally Michalowski, *No Complicity Liability*, *supra* note 98, at 458–70.

267. *See id.* at 470 ("On the other hand, the approach might also have unfair consequences by

law, where the attribution of responsibility usually depends on an analysis of the facts of each case, not on a categorical approach that excludes liability for a whole species of acts based on their abstract nature.

It might well be that military vehicles have a more substantial effect on the commission of violations, that a causal link between the sale and the violation can be shown more easily in that case, or that the necessary mens rea might be more easily discerned. However, while it might be easier to link vehicles with extrajudicial killings if they have a military customization that makes their use for harmful purposes more likely while such a link might be more difficult to establish where vehicles do not have such specifications, it is doubtful that the imposition of liability is justified by the abstract nature of the act or product, rather than by its effect on the commission of the violations that were carried out. Where the impact of the sale on the violations is the same, it is difficult to see on what grounds the two sales should be distinguished at the actus reus level, the function of which is to establish the necessary link between the act of assistance and the commission of the principal offense.[268] In the example of the sale of vehicles, it should instead be necessary to demonstrate in each case that the sale of a military vehicle had a substantial effect on the commission of the crimes, or, conversely, that the sale of ordinary vehicles did not. Otherwise there is a risk of both under- and overinclusiveness.

A risk of underinclusiveness would exist because a considerable gap in corporate accountability would be created, encouraging, or at least providing no incentive to refrain from, business transactions that facilitate gross human rights violations other than by providing the direct means for their commission. Such an approach would imply that it is acceptable and legitimate for corporations to provide business partners with inherently neutral goods or services, if they know, or potentially even wish, that they make a substantial contribution to the commission of gross human rights violations.

Such an approach might also have unfair consequences of over-inclusiveness by presuming causation where inherently dangerous goods are provided to a regime that commits grave human rights violations, even if the transaction was not prohibited and might even have been politically encouraged, without any showing that the provision of the product, did, in fact, have a substantial effect on the commission of human rights violations. According to the court in In re *South African Apartheid Litigation*, "[a]lthough such goods may have legitimate uses, that issue is addressed by the *mens rea* element."[269] At first sight it might seem odd that the use of a product should be a mens rea rather than an actus reus concern. The court must have had in mind an assumption that the provision of inherently harmful products satisfies the actus reus requirement. Complicity liability can then only be avoided if the corporation demonstrates that it was unaware of the harmful use the business partner would make of the inherently harmful products. The fine line

presuming causation where inherently dangerous goods are provided to a regime that uses them to commit grave human rights violations.").

268. Norman Farrell, *Attributing Criminal Liability to Corporate Actors: Some Lessons from the International Tribunals*, 8 J. INT'L CRIM. JUST. 873, 891 (2010) (observing that "there does not seem to be any principled legal reason to preclude contributions such as funds, which may substantially contribute, but with more links, in the causal chain between the assistance and the crime").

269. *In re* South African Apartheid Litig. 617 F. Supp.2d 258, n.157.

between acceptable business transactions and complicity liability would rest on mens rea alone in those cases.

A categorical approach to the actus reus as suggested in In re *South African Apartheid Litigation* thus leads to arbitrary results. The imposition of liability should instead depend on a thorough analysis in each case in which complicity in gross human rights violations is alleged. This was also the conclusion of the Appeals Chamber of the SCSL in *Taylor,* which regarded a case-by-case approach for determining the substantial effect of an act of assistance as both necessary and sufficient in order to establish the relevant link between the assistance and the principal offense.[270] The tribunal rejected a categorical approach to determining the actus reus of aiding and abetting liability, even in cases of dual purpose acts that might include commercially-based activities.[271] Unlike the approach in In re *South African Apartheid Litigation*, the tribunal in *Taylor* held that the focus of the analysis had to be on the specific effect of the assistance in each case, not on an abstract assessment of its dangerousness.[272] It rightly pointed out that "perfectly innocuous items, such as satellite phones, could be used to assist the commission of crimes, while instruments of violence could be used lawfully. The distinction between criminal and non-criminal acts of assistance is not drawn on the basis of the act in the abstract, but on its effect in fact."[273] The focus of the liability analysis therefore needs to be on the actual effect of the assistance on the crime, not on its potential effect based on the nature of the product or service provided.

Instead of developing a checklist of factors that need to be met, or identifying situations in which liability is always excluded, the SCSL made clear that the analysis would always have to take account of the circumstances as a whole, as the culpability of an accomplice can only be determined based on an assessment of all relevant factors in each case.[274] Where the assistance was provided to a group or organization, for example, the tribunal in *Taylor* did not conclude that the actus reus of aiding and abetting could not be satisfied unless the group exclusively dedicated itself to pursuing criminal purposes. Rather, this depends on the circumstances, and one important factor for finding substantial effect might be that the assistance was given in the context of widespread and systematic crimes, rather than one isolated criminal act.[275] Nevertheless, the court in *Blankenship* rightly emphasized that "[s]ometimes a single transaction extends over a substantial period and is the equivalent of enduring supply,"[276] as in *Giovannetti*, which involved premises leased for the purpose of illegal gambling.[277] This confirms the main message in *Taylor* that in the end, the overall assessment will depend on the circumstances of each case.

Where the assistance provided was not the only source of assistance the principal offender obtained, the effect of the accomplice's act on the commission of

270. Prosecutor v. Taylor, Case No. SCSL-03-01-A, Appeals Judgment, paras. 390–91 (Special Court for Sierra Leone Sept. 26, 2013).

271. *Id.* paras. 393–95.

272. *Id.* para. 395.

273. *Id.*

274. *Id.* paras. 390–91.

275. *Id.* para. 391.

276. United States v. Blankenship, 970 F.2d 283, 287 (7th Cir. 1992).

277. United States v. Giovanetti, 919 F.2d 1223, 1225 (7th Cir. 1990).

the crimes overall is regarded as crucial. It is consequently important to assess in each case the effect of the assistance on the crime, based on the quantity and quality of the assistance, including its timing and whatever other factors might be relevant in each case. As highlighted in *Perišić*, substantial effect can, for example, be established based on the volume of assistance.[278] And in his dissent in *Perišić*, Judge Liu opined that substantial effect depends on factors such as "the magnitude, critical importance, and continued nature of the assistance."[279]

In light of *Taylor*, an analysis of the actus reus of corporate complicity liability would require a thorough examination of all the factors of the individual case. Where, for example, money is provided to a regime that commits gross human rights violations, liability would depend on how substantially the money assisted the violations carried out by the regime, in light of all the different income sources it had at its disposal. Similarly, regarding the sale of military vehicles, liability would depend on the systematic nature of the violations carried out with the vehicles' help and how important the vehicles provided were for the commission of the offenses, among other factors. At the same time, given that no showing of direct assistance is necessary, no link between the actual goods sold and the violation carried out would need to be established, so a defendant could not avoid liability by alleging that massacres carried out could not be linked to the precise vehicle sold, or the money lent.

Even though the definition of "substantial effect" on a case-by-case basis is clearly not easy and straightforward, such an analysis nevertheless provides the most convincing way to establish liability at the actus reus level. Furthermore, it cannot easily be avoided, as it is even relevant in determining whether the mens rea requirement is satisfied if the purpose standard is applied, since many courts link the inference of purpose to the substantiality of the assistance. Accordingly, even the adoption of a heightened mens rea standard of purpose does not make the potentially complicated substantiality analysis obsolete, unless, as in some ATS cases, courts apply it in such a way that a finding of purpose is effectively excluded in cases in which the act of assistance was a commercial or business-related activity that was primarily motivated by business interests.

B. The Mens Rea Analysis

Some courts in ATS litigation[280] and some U.S. criminal courts[281] impose restrictions at the mens rea level and regard a particularly blameworthy mental state in the form of purpose as the "more" that needs to be present in order to turn an otherwise lawful and acceptable business activity into a reprehensible act of complicity. The ICTY Appeals Chamber's decision in *Perišić* applied—though at the actus reus level—a comparable approach, in cases of dual-purpose acts that can only result in liability if they were rendered with the aim of furthering unlawful

278. Prosecutor v. Perišić, Case No. IT-04-81-A, Appeals Judgement, paras. 56, 68 (Int'l Crim. Trib. for the Former Yugoslavia Feb. 28, 2013).

279. *Id.* para. 9 (Liu, J., dissenting in part).

280. *E.g.*, Presbyterian Church of Sudan v. Talisman Energy, Inc., 582 F.3d 244, 258–59 (2d Cir. 2009).

281. *E.g.*, United States v. Falcone, 109 F.2d 579, 581 (2d Cir. 1940); United States v. Peoni, 100 F.2d 401, 402 (2d Cir. 1938).

purposes.[282] In order to assess whether this is the test according to which liability for corporate complicity in human rights violations should be determined, it is important to be clear about the reasons behind and the implications of such an approach.

1. The Relevance of the Nature of the Act for Defining and Inferring Purpose

The commercial nature of the act of assistance is relevant both as a justification for imposing a mens rea standard of purpose and for how the purpose test is applied in individual cases. Under the ATS, courts are prepared to infer purpose to facilitate violations carried out by the principal from the knowing act of providing assistance that is either in itself unlawful or goes beyond a mere business activity, even when profit is the primary aim.[283] On the other hand, they refuse to infer purpose from engagement in ordinary commercial activities undertaken with the knowledge that they will assist the commission of human rights violations.[284] Indeed, the fact that these activities are usually business motivated speaks against an inference of purpose for these courts.[285]

Courts that apply a purpose test recognize that the purpose to facilitate the commission of the offense can, and in fact often must, be inferred from the act of assistance itself or from the surrounding circumstances.[286] Short of a confession with regard to the accomplice's mens rea, the mental element will have to be established based on circumstantial evidence, which in most cases will make it necessary to resort to the aider and abettor's knowledge with regard to the consequences of the act of assistance.[287] As courts are not prepared to infer purpose from the knowing undertaking of ordinary commercial transactions, this approach largely seems to exclude any corporate complicity liability outside of already objectively unlawful business transactions.

An exception to this approach can be found in *Doe I v. Nestle*, where the court was prepared to infer purpose even though the act of assistance—providing assistance to cocoa farmers—was not unlawful, and was carried out with the primary purpose of profit and not with the desire to harm the children who worked on these farms under conditions of slavery.[288] Thus, in *Nestle*, just as in *Talisman*,[289] the aim pursued by the corporation was that of enhancing its profits, even if that meant assisting the commission of gross human rights violations. The court nevertheless

282. *Perišić*, Case No. IT-04-81-A, para. 44.

283. Sarei v. Rio Tinto, PLC, 671 F.3d 736, 766–67 (9th Cir. 2011) (Schroeder, J., plurality opinion), *vacated*, 133 S. Ct. 1995 (2013); *In re* Chiquita Brands Int'l, Inc., 792 F. Supp. 2d 1301, 1349 (S.D. Fla. 2011).

284. *See* discussion *supra* Part I.B.6.

285. *See, e.g.*, *Talisman*, 582 F.3d at 262 (finding that because there were "benign and constructive purposes" for the projects, there was no purpose to commit human rights violations).

286. *Id.* at 264; *see also* Khulumani v. Barclay Nat'l Bank, Ltd., 504 F.3d 254, 276 n.11 (2d Cir. 2007) (Katzmann, J., concurring) (noting that the intent to purposefully facilitate illegal activities "could be inferred" under certain circumstances).

287. *See* Cassel, *supra* note 13, at 312 (arguing for an interpretation of the purpose test that allows purpose to be inferred from knowledge).

288. Doe I v. Nestle USA, Inc., 766 F.3d 1013, 1024–26 (9th Cir. 2014).

289. *Talisman*, 582 F.3d at 262.

distinguished *Talisman* on the basis that in *Nestle*, the corporation allegedly directly benefited from the violations, i.e., child slave labor, as it lowered its production costs and raised its profits.[290] In *Talisman,* on the other hand, the corporation did not receive such benefits, according to the court in *Nestle*.[291]

However, Talisman clearly benefited from the military protecting its investment.[292] Whether or not it benefited from the human rights violations carried out in order to provide this protection might depend on whether it would have been possible in the specific context of this investment in a conflict zone for the military to provide Talisman with the protection in a lawful way. More importantly, however, the court in *Talisman* made very clear that in cases of otherwise legitimate commercial transactions the mens rea of purpose was only met when the corporation desired the human rights violations to take place.[293] This is difficult to reconcile with the finding in *Nestle* that the defendants purposefully supported child slavery,[294] even though they "did not have the subjective motive to harm children."[295] These inconsistencies could have been avoided had the court in *Nestle* applied a knowledge standard of mens rea, instead of leaving this question open. Alternatively, the court could have clarified that purpose can, in fact, be inferred from the knowing provision of assistance without any need to show a primary purpose in the form of a desire to assist with bringing about the violations. This would, however, have required the court to deviate from the purpose standard in the form of motive adopted in *Talisman*.

The inconsistencies in the application of the purpose standard are also evident when comparing the *Chiquita* and *Kiobel* cases. In *Chiquita*, the court seems to infer a desire to bring about the violations from the illegitimacy of the underlying activities, even though it specifically states that the corporation was primarily pursuing its business interests and driven by profit.[296] It might be easy to deduce knowledge in such a case, but to infer a purpose directed at the commission of human rights violations in *Chiquita* seems as fictitious as to deny the presence of such a purpose in *Kiobel* where Shell, in pursuit of its business interests, knowingly facilitated them.[297] It is in most cases simply not possible to know what, beyond furthering its business interests, motivated the corporate activities. A mens rea standard in which knowledge serves as the basis on which to determine the individual's state of mind might then "lead to a more objectified interpretation of the factual findings"[298] than a standard that requires inferences regarding the accessory's primary, secondary, exclusive, or other purposes that motivated the act of participation. Moreover, "[t]he distinction of an aim pursued and a known

290. *Nestle*, 766 F.3d at 1024.

291. *Id.*

292. *See Talisman*, 582 F.3d at 261–63 (explaining the allegations that Talisman was assisting the government, and, in turn, was benefitting from the government's creation of a "buffer zone" around the Talisman oil fields by "displacing huge numbers of civilians," allowing Talisman to operate).

293. *Id.* at 263–64.

294. *Nestle*, 766 F.3d at 1025–26.

295. *Id.* at 1025.

296. *In re* Chiquita Brands Int'l, Inc., 792 F. Supp. 2d 1301, 1349 (S.D. Fla. 2011).

297. Kiobel v. Royal Dutch Petroleum Co., 621 F.3d 111, 193 (2d Cir. 2010) (Leval, J., concurring in the judgment).

298. Hans Vest, *A Structure-Based Concept of Genocidal Intent*, 5 J. INT'L CRIM. JUST. 781, 795–96 (2007).

consequence conclusively connected with such aim is not basic enough to justify a different legal result: both cases should be handled equally."[299]

This brings into focus another problem of the purpose approach. Given that those courts that applied a purpose test under the ATS tended to bypass any actus reus analysis, the motive with which the act of assistance was carried out becomes the main point of reference for distinguishing between the acceptable and the unlawful. However, this is unsatisfactory, as it is doubtful that the motive behind the act of assistance can be determined with sufficient certainty to provide a reliable criterion for delineating complicity liability.

This concern is echoed in domestic criminal law cases. In this context, courts also attach significance to the nature of the assistance and are more easily prepared to infer intent where the goods were inherently harmful, their sale or resale restricted, or the transactions themselves dubious.[300] The nature of the assistance thus influences the amount of evidence needed to establish knowledge and intent.[301] Nevertheless, some courts expressed doubts that the criteria to determine the circumstances in which an inference of intent to join was permissible were delineated clearly enough.[302] In order to overcome this and other problems with the mens rea test of purpose, such as impunity in cases of assisting serious offenses[303] or dangerous acts,[304] some courts introduced a substantiality element for the act of assistance and suggested that "where the evidence of the defendant's intent must be inferred from the aid given," a case might be made to modify the analysis by focusing instead "on the amount of assistance knowingly given."[305] Indeed, it was pointed out that "[m]aterial assistance deliberately given is itself evidence of intent."[306] Most courts use this approach for determining the mens rea, rather than for an actus reus analysis, and infer both knowledge and intent from the substantial nature of the assistance, while rejecting such an inference where the assistance is trivial.[307] Thus, while courts in the ATS context refused to infer intent based on the substantial nature of the assistance in cases of ordinary commercial transactions, in domestic cases courts felt that it was justified to make such an inference.

---

299. *Id.* at 789 (emphasis omitted).

300. *See* Direct Sales Co. v. United States, 319 U.S. 703, 711–12 (1943) (describing factors taken into account to determine sellers' knowledge of whether goods will be used unlawfully).

301. *Id.*

302. United States v. Blankenship, 970 F.2d 283, 286 (7th Cir. 1992).

303. United States v. Fountain, 768 F.2d 790, 798 (7th Cir. 1985).

304. *See* United States v. Zafiro, 945 F.2d 881, 887–88 (7th Cir. 1991) (dictum) ("It might be better in evaluating charges of aiding and abetting to jettison talk of desire and focus on the real concern, which is the relative dangerousness of different types of assistance . . . .").

305. United States v. Irwin, 149 F.3d 565, 572 (7th Cir. 1998).

306. *Id.* (emphasis omitted). *See also* Tenore v. Am. & Foreign Ins. Co. of N.Y., 256 F.2d 791, 794–95 (7th Cir. 1958) (discussing intent in the context of insurance and stating that "[i]f a false statement is knowingly made by the insured with regard to a material matter, the intent to defraud will be inferred").

307. *See, e.g.*, *Fountain*, 768 F.2d at 798 (comparing the more trivial act of assisting prostitution through supplying a dress and the more serious act of assisting murder by providing the murder weapon in conducting mens rea analysis).

2. Analysis of the Reasons for Adopting a Purpose Test in U.S. Criminal Law

Courts have adopted a mens rea standard of purpose in the domestic context as a reaction to the lack of a substantiality or materiality requirement at the actus reus level;[308] the mens rea standard ensures that not every sale of a lawful good to another person can result in complicity liability if the buyer then uses it for unlawful purposes. The main reason behind promoting a mens rea standard of purpose seems to be "to promote autonomy by precluding criminal impediments to otherwise lawful activities that depend on social interaction, especially business."[309]

The question, nevertheless, is whether the balance between not inhibiting lawful activities and deterring crime is best achieved by imposing a mens rea test of purpose, as it is doubtful that the test really delivers what it seems to promise. Indeed, in the domestic cases discussed in this Article, it is difficult to see why, as the courts assume, the prevention of activities is better achieved by imposing a mens rea test of desire than one of knowledge.[310] It might well be right that not much would be gained by imposing liability in the prostitution cases, while it would be justified to hold the seller of the gun liable. The effect of selling a dress or an address book to a prostitute on the commission of the crime of prostitution is in all likelihood minor, whereas the sale of a gun that is used for murder has a much more profound impact on the commission of the principal offense. However, the difference between the two cases seems to lie at the actus reus and not the mens rea level. In one case, the assistance is crucial for committing the crime; in the other its potential to further the crime is so minimal that it is difficult to establish a link between the crime and the assistance.

Whether or not the different nature of the assistance in the two cases might also impact the possibility of inferring intent to further the crime seems much less relevant. Indeed, given the courts' focus on deterrence in these cases, it is not obvious what, exactly, would be gained by criminalizing the sale of the dress even if the seller acted with the purpose to assist with prostitution, unless, exceptionally, the dress was a significant factor in facilitating the crime. The furtherance of prostitution would not be any greater if the seller acted with the relevant purpose. Similarly, regarding Judge Leval's example in *Kiobel* of Hitler's shoemaker,[311] he could be an aider and abettor of Hitler's crimes if he expressed his desire that the shoes assist him with his crimes. However, little would be achieved if liability depended decisively on the shoemaker's motives, as it is rather unlikely that the shoes will have had any effect on the crimes committed.[312]

---

308. Weiss, *supra* note 200, at 1483 (using the "bad purpose and purposeful intent approaches protect[s] the marginally involved participant").

309. James G. Stewart, *The End of "Modes of Liability" for International Crimes*, 25 LEIDEN J. INT'L L. 165, 191 (2012).

310. *See* Weiss, *supra* note 200, at 1484 (asserting the superiority of the knowledge test for deterrence purposes).

311. Kiobel v. Royal Dutch Petroleum Co., 621 F.3d 111, 158 (2d Cir. 2010) (Leval, J., concurring in the judgment).

312. *See* Sykes, *supra* note 8, at 2203 ("Instead, civil aiding and abetting liability is most likely to be useful when it penalizes actors who have a meaningful capacity to exert control or impose restraint on the primary wrongdoer.").

In the U.S. criminal case of *Zafiro,* the court appreciated this and opined that "[i]t might be better in evaluating charges of aiding and abetting to jettison talk of desire and focus on the real concern, which is the relative dangerousness of different types of assistance . . . ."[313] What would matter then is no longer the desire of the accomplice to further the principal offense, but rather whether the assistance is sufficiently essential to impose complicity liability and whether the accomplice knew this. The liability test would thus be transformed to a test of providing knowing assistance of more than a trivial nature. *Hanauer v. Doane* nicely expressed some other reasons in support of a knowledge test for mens rea:

> Can a man furnish another with the means of committing murder, or any abominable crime, knowing that the purchaser procures them, and intends to use them, for that purpose, and then pretend that he is not a participator in the guilt? . . . [No, h]e cannot be permitted to stand on the nice metaphysical distinction that, although he knows that the purchaser buys the goods for the purpose of aiding the rebellion, he does not sell them for that purpose.[314]

Since *Hanauer v. Doane* was decided, the knowledge standard has clearly lost traction with U.S. courts, but this analysis of the criminal cases has shown that courts often do, in fact, apply a substantial assistance plus knowledge test, even though they claim to insist on purpose as the necessary mens rea standard.

3. Analysis of the Reasons for Adopting a Purpose Standard in Corporate Complicity Cases

In the context of corporate liability under the ATS, where the actus reus requires an act of assistance that has a substantial effect on the commission of the violation of the law of nations, the adoption of the purpose test reflects the view that legitimate commercial transactions are only transformed into blameworthy acts of complicity where the abuses were desired by the corporation and the facial harmlessness of the act is counterbalanced by a particularly reprehensible state of mind. The approach to the mens rea test both in *Talisman* and in Judge Leval's concurring opinion in *Kiobel* was at least partly motivated by the concern that without a strict mens rea standard of purpose liability would stretch too far, expressing a clear distrust in the possibility of limiting liability sensibly at the actus reus level in cases of commercial transactions. The purpose test might then be regarded as an appropriate tool to limit liability if the claims are perceived as unjustified interference in legitimate business decisions. In this vein, courts have expressed concerns that litigation would allow "private parties to impose embargos or international sanctions through civil actions in United States courts,"[315] and dissuade companies from carrying out business with regimes that have "less than stellar human rights records."[316]

---

313. United States v. Zafiro, 945 F.2d 881, 887–88 (7th Cir. 1991) (dictum).

314. Hanauer v. Doane, 79 U.S. 342, 347 (1870). *But see* Weiss, *supra* note 200, at 1367 (noting that the knowledge standard was disfavored by subsequent U.S. case law).

315. Presbyterian Church of Sudan v. Talisman Energy, Inc., 582 F.3d 244, 264 (2d Cir. 2009).

316. *In re* S. African Apartheid Litig., 346 F. Supp. 2d 538, 554 (S.D.N.Y. 2004).

Thus, two interrelated reasons seem to lie behind the adoption of a purpose approach: the fear that in the context of commercial activities, the actus reus test is not capable of separating mere commercial transactions with bad actors from those that are worthy of creating complicity liability, and, relatedly, the perception that business transactions with bad actors are legitimate, even where they assist that actor with gross human rights violations, as long as this result was not the primary motive behind the corporate act.

However, to concentrate on the legitimacy of the underlying action or its commercial nature is unhelpful and misleading. Aiding and abetting liability does not require that the act of assistance consist of an activity that is illegitimate in and of itself, regardless of the circumstances of the individual case.[317] What makes a commercial act illegitimate—and gives rise to the imposition of complicity liability—is that in a specific case an act that might under other circumstances be perfectly legitimate assist with carrying out a crime or gross human rights violation and thus meet the actus reus requirements of complicity liability. In the context of the ATS cases, this means that it amounted to practical assistance that had a substantial effect on the commission of gross human rights violations.

While doing business with a State that commits gross human rights violations does not in itself give rise to liability,[318] this is not what the cases against corporations for aiding and abetting are about. In all cases, with more or less detail and different degrees of plausibility, the plaintiffs alleged that certain acts of the defendant corporations had a substantial effect on the commission of gross human rights violations carried out by the governments with which they were doing business. Where the allegations do not meet this standard and simply consist of asserting business transactions between the corporation and the violating state, the claims can be thrown out because of the lack of an actus reus. However, where such an effect can be shown, the act turns from a lawful, harmless, and legitimate activity to an act of aiding and abetting gross human rights violations.

If it is recognized that, at the objective level, the line of acceptable business practices is crossed where substantial assistance with gross human rights violations is rendered, then the issue to be addressed at the mens rea level is not that of how to shield corporations from liability for carrying out legitimate business with states with dubious human rights records. Instead, the question turns into whether liability is only justified if such acts are committed with an exceptionally guilty mind in the form of primary purpose, or whether it is already warranted where the corporation knew of the effect its commercial activities would have on human rights violations. Consequently, the choice of the mens rea standard of purpose reflects the view that it is acceptable that corporations pursue their business interests by knowingly facilitating gross human rights abuses, and in some cases even relying on them for their safety and protection, as long as they do not actively desire or procure them. The perception of commercial transactions as legitimate, even where they have a

317. *See* Stewart (2013(2)), *supra* note 171 ("There is nothing inherently illegal in driving a car away from a bank, but this conduct becomes a paradigmatic example of complicity when it assists a bank robbery.").

318. *In re* S. African Apartheid Litig., 617 F. Supp. 2d 228, 257 (S.D.N.Y. 2009); Mastafa v. Australian Wheat Bd., No. 07 Civ. 7955(GEL), 2008 WL 4378443, at *4 (S.D.N.Y. Sept. 25, 2008); Doe I v. Nestle S.A., 748 F. Supp. 2d 1057, 1090 (C.D. Cal. 2010).

substantial effect on the commission of human rights violations, is thus clearly an important reason behind courts' desire to limit liability.

In the academic discussion, this issue is sometimes linked to the question of the potential virtue of foreign investment even in the most abusive contexts, clearly a divisive issue.[319] Without engaging with this discussion in detail, it should be noted that corporations are free to do business and engage constructively with regimes that commit gross human rights violations on a large scale, as long as they avoid any complicity in these violations.[320] The aim of complicity liability is not to proscribe all business with certain regimes, but rather to discourage the corporate furtherance of the human rights violations they commit.[321] This does not conflict with constructive engagement, as there is nothing constructive about complicity in human rights violations. Conversely, constructive engagement does not give corporations a blank check to be complicit in gross human rights violations carried out by regimes with which they are engaging.[322] Indeed, as Judge Hall rightly suggested in his concurring opinion in *Khulumani v. Barclay National Bank, Ltd.*, "business imperatives [do not] require a license to assist in violations of international law."[323]

Contrary to the message that the adoption of the purpose test conveys, to knowingly assist in the commission of gross human rights violations is not an acceptable business practice,[324] and victims of such practices should not have to endure their consequences without the possibility of obtaining an effective remedy. The Guiding Principles on Business and Human Rights issued by the Special Representative of the Secretary-General on the issue of human rights and transnational corporations and other business enterprises,[325] which were endorsed by the U.N. Human Rights Council, reinforce this in the specific context of human rights responsibilities of corporations.[326] According to Guiding Principle 11, corporations have the responsibility to respect human rights, which "means that they

---

319. *See* Ramsey, *supra* note 26, at 313 (describing the question of investment in countries with abusive regimes as a "troublesome valve judgment").

320. *See, e.g.*, Brian Jacek, *Alien Invasion: Corporate Liability and Its Real Implications under the Alien Tort Statute*, 43 SETON HALL L. REV. 273, 312–14 (2013) (citing Robert Knowles, *A Realist Defense of the Alien Tort Statute*, 88 WASH. U. L. REV. 1117, 1139–40 (2011), for the proposition that "[m]ere investment in an 'authoritarian regime has never been sufficient ground for liability under the ATS'").

321. *See* Richard L. Herz, *The Liberalizing Effects of Tort: How Corporate Complicity Liability under the Alien Tort Statute Advances Constructive Engagement*, 21 HARV. HUM. RTS. J. 207, 210 (2008) ("Without the threat of liability, companies face no consequences for being complicit in the very abuses that constructive engagement is designed to prevent.").

322. *Id.* at 222; *see also* Jacek, *supra* note 320, at 312–14 (allowing a knowledge requirement "create[s] an incentive for corporations to implement internal compliance structures within the corporation to prevent and limit liability"); Michalowski, *No Complicity Liability*, *supra* note 98, at 521–22 ("[C]onstructive engagement cannot give corporations a blank check to be complicit in gross human rights violations carried out by regimes with which they are engaging.").

323. Khulumani v. Barclay Nat'l Bank Ltd., 504 F.3d 254, 289 (2d Cir. 2007) (Hall, J., concurring).

324. *See, e.g.*, *id.* at 289 (dismissing the idea that "business imperatives require a license to assist in violations of international law"); Prosecutor v. Furundžija, Case No. IT-95-17/1-T, Judgement, paras. 238, 245 (Int'l Crim. Trib. for the Former Yugoslavia Dec. 10, 1998) (following the holding of the *Zyklon B Case*); The Zyklon B Case, 1 LAW REPORTS OF TRIALS OF WAR CRIMINALS 93, 94, 102 (1947) (finding that the knowing provision of the poison gas to those committing gross human rights violations subjects the defendants to liability). See also the discussion *supra* in Part IV.A.

325. Ruggie, *Guiding Principles*, *supra* note 1, cmt. to principle 17.

326. *See generally id.*

should avoid infringing on the human rights of others and should address adverse human rights impacts with which they are involved."[327] This responsibility includes the avoidance of complicity in human rights violations carried out by their business partners.[328] The Guiding Principles impose on corporations the responsibility to carry out human rights due diligence in order to become aware of the human rights impacts of their business operations (Guiding Principle 17), including the risk of complicity.[329] Due diligence requires proactive behavior to "become aware of, prevent and address adverse human rights impacts."[330] These responsibilities thus go even further than the knowledge standard, as corporations cannot hide behind their ignorance.[331] While not legally binding on the corporations, the Guiding Principles are widely recognized[332] and show that knowing complicity in human rights violations is not regarded as an acceptable and legitimate business practice and that victims of such practices should not be left without a remedy.[333]

Judge Leval forcefully criticized the majority in *Kiobel*, which squarely rejected civil liability of corporations under the ATS, on the grounds that such a rule has the effect "to immunize the profits earned from the most heinous acts known to mankind" and "operates to the detriment of the objective of international law to protect fundamental human rights."[334] However, the application of the purpose test has a similar effect when it provides impunity to corporations that knowingly facilitated gross human rights violations for the purpose of profit maximization. Indeed, it regards the pursuance of commercial interests as legitimate even where it furthers gross violations of the human rights of others, as long as the corporation is simply indifferent to them or might prefer that they do not occur.[335] Given that this will be the situation in the vast majority of corporate complicity cases, Chief Justice Jacobs might well have been right when commenting in the *Kiobel* decision denying an en banc rehearing of the Second Circuit's decision that, if the relevant mens rea test is one of purpose, the question of whether or not the ATS provides for a remedy in cases of corporate complicity "is one of no big consequence"[336] as this excludes the possibility of successfully arguing a case of corporate liability under the ATS so effectively that "[t]he incremental number of cases actually foreclosed by the majority opinion in *Kiobel* approaches the vanishing point."[337] As a consequence, under the purpose test, there is no incentive for corporations to refrain from knowingly aiding and abetting abuses where to do so would be beneficial for business. Instead, individuals and corporations will be isolated from the known and

327. *Id.* principle 11.

328. *Id.* principle 17 & cmt. *See also* Ruggie, *Clarifying the Concepts*, *supra* note 1, paras. 26, 71 (stating that corporations should practice due diligence to avoid complicity in human rights violations).

329. Ruggie, *Guiding Principles*, *supra* note 1, cmt. to principle 17.

330. Ruggie, *Clarifying the Concepts*, *supra* note 1, para. 23.

331. For a discussion *see, e.g.*, Radu Mares, *Defining the Limits of Corporate Responsibilities Against the Concept of Legal Positive Obligations*, 40 GEO. WASH. INT'L L. REV. 1157, 1205–06 (2009).

332. *Id.* at 1165 n.26.

333. Ruggie, *Guiding Principles*, *supra* note 1, principle 22 & cmt. (suggesting in this respect that "[w]here business enterprises identify that they have caused or contributed to adverse impacts, they should provide for or cooperate in their remediation through legitimate processes").

334. Kiobel v. Royal Dutch Petroleum Co., 621 F.3d 111, 159 (2d Cir. 2010) (Leval, J., concurring in the judgment).

335. Michalowski, *The Mens Rea Standard*, *supra* note 13, at 272.

336. *Id.* at 240 (quoting Kiobel v. Royal Dutch Petroleum, 642 F.3d 268, 270 (2d Circ 2011)).

337. *Id.* (quoting *Kiobel*, 642 F.3d at 271).

foreseen consequences of their actions as long as they are indifferent to their occurrence and motivated by business or other interests.

The latter is, of course, precisely what proponents of the purpose/specific direction approach want to achieve. In support of the approach in *Perišić*, for example, Professor Kevin Jon Heller has commented that otherwise, if

> individuals who interact with organizations engaged in both lawful and unlawful acts . . . are aware of the unlawful acts, they cannot provide the organization with any assistance that might end up facilitating them — even if they do not intend to facilitate those acts, and even if they do everything in their power to prevent their facilitation.[338]

Similar issues could arise in the case of corporations that provide regimes that have very bad human rights records with goods or services that can be used to commit human rights violations. The above statement is, nevertheless, not entirely true, unless the applicable liability standard is that of knowing provision of any form of assistance, which is neither the case in international criminal law nor under the ATS. In both cases, the actus reus requires the provision of assistance that has a substantial effect on the commission of the principal offense. Nevertheless, Heller tries to show the, in his view, untenable consequences of a liability standard of knowing substantial assistance by citing the example of providing weapons to rebels in Syria who lawfully fight against the Assad regime, despite widespread knowledge that these rebel groups commit war crimes and crimes against humanity.[339] In his view, governments and organizations that provide weapons in these circumstances would incur aiding and abetting liability "[u]nless . . . the actus reus of aiding and abetting requires proof that the defendant specifically directed his assistance to an organization's unlawful acts."[340] With a specific direction requirement—or, presumably, a mens rea test of purpose—in place, "as long as the British government and the CIA do everything they can to ensure that their provision of weapons facilitate only lawful rebel actions, they cannot be held legally responsible for any international crimes committed, despite their best efforts, with those weapons."[341]

A finding that the assistor did everything possible "to ensure that their provision of weapons facilitate only lawful rebel actions" would clearly go a long way to show that there was no specific direction to assist the unlawful use.[342] However, the specific direction requirement isolates the assistor from the unlawful acts and their consequences, as long as a reasonable conclusion that the assistance was provided for lawful purposes is possible, regardless of the presence or absence of attempts to ensure that the assistance provided will only be put to a lawful use. Just like a purpose test of mens rea, it thus allows the individual or corporation providing assistance to evade liability as long as they can show that they did not, in fact, intend the logical consequences of their acts to come about. As Judge Liu emphasizes in his forceful partial dissent in *Perišić*, the adoption of the specific direction requirement

338. Heller, *supra* note 171.
339. *Id.*
340. *Id.*
341. *Id.*
342. *Id.*

"risks undermining the very purpose of aiding and abetting liability by allowing those responsible for knowingly facilitating the most grievous crimes to evade responsibility for their acts."[343]

The *Zyklon B* case in which industrialists were accused of supplying the Nazis with large quantities of the poison gas Zyklon B that was used for the mass killings of concentration camp victims—but also had lawful uses—provides a good example for demonstrating the unacceptable consequences of applying a purpose test.[344] As industrialists, the defendants' primary purpose was presumably to make a profit with the gas they sold to the Nazi regime. Indeed, the Trial Chamber in *Prosecutor v. Furundzija* stressed that "their purpose was to sell insecticide to the SS (for profit, that is a lawful goal pursued by lawful means)."[345] However, the lawfulness of the underlying transactions was regarded as irrelevant when determining the defendants' culpability, and rightly so.[346] It would be difficult to justify holding them accountable for the atrocities they knowingly facilitated in pursuance of their business interests only if they desired the killings to take place, while indifference to the effects of their actions, or even repugnance, should exonerate them, if they nevertheless knowingly provided the gas.[347]

As this analysis has shown, the purpose test of mens rea faces many objections, spanning from the need to infer purpose in most cases from knowledge, to the undesirable consequences of a test that regards as legitimate the knowing provision of substantial assistance to further crimes or human rights violations, as long as the main objective of the act is business oriented.

CONCLUSION FOR DEVELOPING CRITERIA FOR DETERMINING CORPORATE COMPLICITY LIABILITY

This Article has shown that the commercial and routine nature of an activity does not preclude complicity liability. The question is rather under what circumstances, and according to which criteria, complicity liability can be triggered in the context of commercial activities. In particular, does the commercial context require or at least justify applying separate, more restrictive liability criteria than those used to determine complicity liability outside of this specific context?

In the ATS cases, many courts answered that question in the affirmative and roughly distinguished two situations: (1) corporate acts that are facially lawful and consist of commercial transactions, such as the sale of goods or provision of services

343. Prosecutor v. Perišić, Case No. IT-04-81-A, Appeals Judgement, para. 3 (Int'l Crim. Trib. for the Former Yugoslavia Feb. 28, 2013) (Liu, J., dissenting in part).

344. The Zyklon B Case, 1 LAW REPORTS OF TRIALS OF WAR CRIMINALS 93, 94 (1947),

345. Prosecutor v. Furundžija, Case No. IT-95-17/1-T, Judgement, para. 238 (Int'l Crim. Trib. for the Former Yugoslavia Dec. 10, 1998).

346. *See* The Zyklon B Case, 1 LAW REPORTS OF TRIALS OF WAR CRIMINALS 93, 102 (sentencing defendants to death for sale of insecticide to the SS, presumably based on their knowledge that it would be used to kill human beings).

347. *See* Khulumani v. Barclay Nat'l Bank, 504 F.3d 254, 290 (2d Cir. 2007) (Hall, J., concurring) ("The Zyklon B Case provides a clear example of when liability would attach . . . when a defendant provides 'the tools, instrumentalities, or services to commit [human rights] violations with actual . . . knowledge that those tools, instrumentalities or services will be (or only could be) used in connection with that purpose.'" (citation omitted)).

that are used by a third party to commit human rights violations; and (2) corporate behavior that is itself unlawful and clearly falls outside of legitimate business transactions, such as incitement to commit crimes or human rights violations, or paying paramilitary or terrorist groups to protect corporate investments. In the first scenario, liability was only found if either the assistance was inherently harmful or provided the direct means for carrying out the violations, or where the defendant acted with the direct purpose of assisting their commission. In the second type of cases, the courts easily find the line between legitimate commercial activities and those that trigger corporate complicity to be crossed, as the unlawfulness of the corporate activity will in most cases mean that it cannot be associated with ordinary commercial dealings.

However, as argued in Part IV, even where it can be easily and uncontroversially determined that the act of assistance was unlawful or exceeded the commercially acceptable, liability should still require establishing a link between the act and the violations, and it is still necessary to establish the relevant mens rea.[348] At the same time, aiding and abetting liability does not require that the act of assistance be unlawful on its face. Indeed, "acts which in themselves may be benign, if done for a benign purpose, may be actionable if done with the knowledge that they are supporting unlawful acts."[349] This is why someone who drives the getaway car after a bank robbery can be held liable as an accomplice, even though the act of driving is clearly, in principle, lawful. Basing the determination of the liability standards in corporate complicity cases on the lawful, ordinary, or routine nature of the act of assistance is therefore flawed.

Instead of applying the existing liability standards to determine the lawfulness of the underlying act in the circumstances of each case (which is how complicity cases are dealt with outside of the commercial context), it seems that the courts have approached the question the wrong way and allowed the definition of liability to be guided by the perceived legitimacy of the commercially motivated act of assistance and adapted the applicable liability standards in light of this. This is not to suggest that liability standards can or should be determined in isolation from the reality of, and the policy considerations applicable in, any given situation. Nevertheless, if the commercial nature of an act that otherwise meets the criteria of complicity liability is the primary reason to adapt and lower liability standards—which in many cases might result in exempting corporate actors from liability—this would require a justification that goes beyond the mere fact of the commercial nature or motivation of the act. As this Article has demonstrated, none of the explanations that have been advanced satisfactorily substantiates such a claim.

It does not follow, however, that the commercial nature of the act of assistance might not be of relevance when determining complicity liability. While not determinative, whether or not the act of assistance consisted of the provision of routine and lawful commercial services, and whether the goods and services provided were neutral or inherently harmful, might influence the depth of the analysis that is

348. *See supra* Part IV.

349. Almog v. Arab Bank, PLC, 471 F. Supp. 2d 257, 291 (E.D.N.Y. 2007). *See also* Linde v. Arab Bank, PLC, 384 F. Supp. 2d 571, 588 (E.D.N.Y. 2005) (finding that "given plaintiffs' allegations regarding the knowing and intentional nature of the Bank's activities, there is nothing 'routine' about the services the Bank is alleged to provide").

required in each case, both at the actus reus and the mens rea level. One might even reverse the burden of proof where the act of assistance consists of the provision of an inherently harmful product or service or the act of assistance is itself unlawful, to reflect the likelihood that the act of assistance will have a significant effect on the business partners' commission of gross human rights violations, and the likelihood that the corporation knows this.[350] Such a reversal of the burden of proof would need to be rebuttable and open to showing that, in the individual case, the provision of a harmful product did not have a substantial effect on the commission of the crime, or that despite its harmful nature and significant effect, the corporate actor did not have the relevant knowledge to justify the imposition of complicity liability. It would not therefore make a case-by-case analysis obsolete, but rather shift the starting point of the analysis to a presumption in favor of liability in these scenarios.

For the case-by-case analysis, at the actus reus level, it is primarily the nature of the assistance that is of relevance. It might be easier to establish that the provision of inherently harmful goods or services such as the supply of weapons has a substantial effect on the commission of human rights violations such as extrajudicial killings than where money is provided that is used to buy the weapons. However, not every gun sold facilitates an unlawful killing, while money might be lent for the purpose of buying weapons to carry out extrajudicial killings. Thus, all depends on the circumstances of each case, and a thorough analysis is necessary in all situations, even though its intensity might differ depending on the nature of the act of assistance.

Such a case-by-case analysis clearly creates some uncertainty and room for different assessments of individual cases. Some criteria to make such evaluation of the effect of an act of assistance on the commission of human rights abuses, and the substantiality of this effect, more predictable are: the closeness of the accomplice to the commission of the offense; the quality and quantity of the assistance provided; whether the assistance provided the direct means with which the violations were carried out; whether the assistance was provided in the context of a continuing relationship or a one-off transaction or given in the context of systemic rather than isolated violations, to name but a few. Nevertheless, as the discussion of *Taylor* and some of the U.S. criminal cases has shown, such a check list, however comprehensive, can achieve no more than provide points to consider as part of a detailed analysis of the specific circumstances of each case. This, however, is not unusual in law, and courts are used to carrying out such analyses in both criminal and civil cases, based on general liability standards such as substantial effect.[351] Corporations are equally capable, and under the U.N. Guiding Principles on Business and Human Rights are expected,[352] to carry out complicity risk assessments in the context of their commercial relationships.

---

350. For a comparable argument for cases in which the business partner has a particularly bad human rights record, see Michalowski, *No Complicity Liability*, *supra* note 98, at 520 ("Where a regime is widely known to commit gross human rights violations . . . it could be argued that lenders have a heightened due diligence obligation to inquire into the use of money they are lending with respect to the violations taking place.").

351. *See, e.g.*, Gonzales v. Raich, 545 U.S. 1, 17 (2005) (determining whether a regulated activity had a "substantial effect" on interstate commerce such that it could be federally criminalized); Nat'l Fed'n of Indep. Bus. v. Sebelius, 132 S. Ct. 2566, 2585 (2012) (considering whether the failure to have health insurance has a "substantial and deleterious effect on interstate commerce").

352. Ruggie, *Guiding Principles*, *supra* note 1, principle 17 & cmt.

If a thorough actus reus analysis were carried out even in cases in which the alleged assistance consisted of a commercial transaction, aiding and abetting liability would have two filters, one with regard to the act of assistance itself, another concerning the mental state. As particularly the discussion of the prostitution examples in U.S. criminal cases demonstrated, many cases could already be thrown out at the actus reus level, based on the immateriality of the assistance provided. Equally, in the In re *South African Apartheid Litigation* case, the provision of computers to prison authorities might not have had a sufficiently close link to instances of torture to justify a finding that the actus reus of complicity liability is met, unless, based on specific facts in an individual case, such a link can exceptionally be shown. A case-by-case approach to determining the substantial effect of the assistance, coupled with a knowledge test of mens rea, thus does not create limitless corporate complicity liability, as is often alleged.[353]

To address Judge Leval's concern that unless a mens rea test of purpose is applied, Hitler's shoemaker, for example, might be liable for aiding and abetting the atrocious crimes committed by Hitler,[354] it seems that the shoemaker's liability can be much more appropriately excluded at the actus reus than at the mens rea level. It is rather unlikely that the shoes Hitler was wearing had a substantial effect on the crimes he carried out. The shoemaker then cannot be held liable as an accessory to Hitler's crimes, whatever the motives for providing Hitler with shoes. If, however, as Judge Leval suggests, liability depended decisively on the shoemaker's reasons for providing the shoes,[355] he or she could be an aider and abettor of Hitler's crime when making the shoes with the desire that they should assist him with his crimes. This is another demonstration of the fact that even in cases of commercial transactions, the objective and subjective elements of aiding and abetting liability serve different functions, and insubstantial assistance or acts that are too remote to have had a substantial effect on the violations can and should be filtered out at the actus reus level of liability.

At the mens rea level, the commercial nature of the assistance is also potentially highly relevant. It will often be easier to infer knowledge of the business partner's unlawful use of the goods or services provided where a transaction already on its face goes beyond accepted commercial practice, or involves dealing with goods that are particularly prone to unlawful use. Routine commercial transactions, on the other hand, might raise less ground for suspicion with regard to their harmful effects. However, the commercial character of the transaction is not a reason to exclude liability where knowledge can nevertheless be shown, nor does the inherently harmful character of the goods or services automatically give rise to an inference of knowledge with regard to their intended unlawful use. Instead, a thorough analysis based on the facts and circumstances of each case has to be carried out to establish the relevant knowledge.

353. *See* Mares, *supra* note 331, at 1206 (noting that "the threshold of knowledge [required for complicity] might not be very demanding to attract liability").

354. Kiobel v. Royal Dutch Petroleum Co., 621 F.3d 111, 158 (2d Cir. 2010) (Leval, J., concurring in the judgment).

355. *Id.*

Two Nuremberg cases, the *Farben* case[356] and the *Zyklon B* case,[357] provide a good demonstration of how this can work in practice. In both cases industrialists were accused of supplying the Nazis with large quantities of the poison gas Zyklon B that was used for the mass killings of concentration camp members. In the *Farben* case, the defendants were acquitted even though:

> The proof is quite convincing that large quantities of Cyclon-B were supplied to the SS by Degesch and that it was used in the mass extermination of inmates of concentration camps, including Auschwitz. But neither the volume of production nor the fact that large shipments were destined to concentration camps would alone be sufficient to lead us to conclude that those who knew of such facts must also have had knowledge of the criminal purposes to which this substance was being put. Any such conclusion is refuted by the well-known need for insecticides wherever large numbers of displaced persons, brought in from widely scattered regions, are confined in congested quarters lacking adequate sanitary facilities.[358]

The tribunal relied heavily on testimony according to which the use of Zyklon B for the extermination of concentration camp inmates had been "Top Secret" and that none of "the defendants had any knowledge whatever that an improper use was being made."[359] In the *Zyklon B* case, on the other hand, the industrialists were convicted because there was witness testimony to the effect that one of the defendants knew of the criminal use made of the gas,[360] and because the structure of the defendants' enterprise made it implausible that they did not have the relevant knowledge. This shows that even where harmful substances are sold to criminal regimes, inferences of knowledge with regard to their unlawful use are not automatic, but rather depend on an in-depth analysis of all the surrounding circumstances. It can be assumed that the provision of the gas will have had a substantial effect on the commission of the killings, so that the actus reus will have been met in both cases. Nevertheless, the mens rea in the form of knowledge provided a corrective according to which the two cases were distinguished.

Just like the substantial effect requirement at the actus reus level, the mens rea standard of knowledge needs further clarification. In this Article, the assumption, based on the case law discussed, has been that actual knowledge would be necessary, rather than a mere showing that the corporation should have known what effect its commercial transactions would have on the commission of human rights violations.[361] Actual knowledge can be proven if, based on all the circumstances of the case, a reasonable inference can be made that the corporation must have known the

356. The Farben Case (I.G. Farben Case), 8 TRIALS OF WAR CRIMINALS 1 (1952).

357. The Zyklon B Case, 1 LAW REPORTS OF TRIALS OF WAR CRIMINALS 93 (1947).

358. The Farben Case (I.G. Farben Case), 8 TRIALS OF WAR CRIMINALS 1, 1169 (1952).

359. *Id.*

360. The Zyklon B Case, 1 LAW REPORTS OF TRIALS OF WAR CRIMINALS 93, 95–96 (1947).

361. *But see* Doe I v. Unocal Corp., 395 F.3d 932, 953 (9th Cir. 2002) (suggesting that the appropriate test is whether "Unocal knew or should reasonably have known that its conduct—including the payments and the instructions where to provide security and build infrastructure—would assist or encourage the Myanmar Military to subject Plaintiffs to forced labor").

relevant facts.[362] This is different from the "should have known" standard which would be satisfied even if no showing or inference of existing knowledge can be made, but where the accomplice would have had the relevant knowledge had the diligence that could be expected from a reasonable person been exercised.[363] In the context of corporate complicity in human rights violations, an argument can be made for imposing due diligence responsibilities which would require active inquiries into the use the business partner might make of goods or services provided. The imposition of such duties might well raise the cost of business. However, compliance with them has the benefit of reducing the risk of legal claims of corporate complicity "by showing that [the corporation] took every reasonable step to avoid involvement with an alleged human rights abuse,"[364] as well as that of preventing the occurrence of human rights violations through illegitimate uses of corporate products and services. While currently not a legal requirement in most contexts, such due diligence responsibilities are postulated in the U.N. Guiding Principles on Business and Human Rights.[365] However, their scope has so far not been outlined clearly.[366]

Another mens rea related question that still needs refining is what, precisely, the accomplice needs to know to incur liability.[367] It has been suggested that while the aider and abettor would not "necessarily have to know all factual (e.g., date, location, offender, victim) or normative (e.g., gravity) details of the principal crime . . . there should be a requirement that the accessory, at minimum, knows about the 'offence' that he facilitates."[368] The ad hoc international criminal tribunals, while requiring knowledge "that the acts performed by the aider and abettor assist [in] the commission of the specific crime of the principal,"[369] nevertheless clarify that knowledge of "the precise crime that was intended and which in the event was committed" is not necessary.[370] Rather, knowledge that "one of a number of crimes will probably be committed" is sufficient.[371] Whether or not corporations acted with the necessary mens rea would then depend on whether they knew of the types of crimes to be committed, and of the effect of their assistance on these crimes.

As the International Commission of Jurists explains, a corporation that knows "that the equipment the business is selling is likely to be used by a buyer for one of a number of crimes would not escape liability because there is uncertainty as to the exact crime intended."[372] In many of the corporate complicity cases such knowledge can be inferred either because the human rights violations committed by a regime are well-documented and generally known, or because they came to the knowledge

362. *In re* S. African Apartheid Litig., 617 F. Supp. 2d 228, 265 (S.D.N.Y. 2009).

363. Mares, *supra* note 331, at 1205–06.

364. Ruggie, *Guiding Principles*, *supra* note 1, principle 17 & cmt.

365. *Id.*

366. For discussion, see generally Michalowski, *Due Diligence*, *supra* note 5.

367. For discussion, see generally Michalowski, *The Mens Rea Standard*, *supra* note 13.

368. Burchard, *supra* note 57, at 939.

369. Prosecutor v. Blaškić, Case No. IT-95-14-A, Appeals Judgement, para. 45 (Int'l Crim. Trib. for the Former Yugoslavia July 29, 2004) (quoting Prosecutor v. Vasiljević, Case No. IT-98-32-A, Appeals Judgement, para. 102 (Int'l Crim. Trib. for the Former Yugoslavia Feb. 25, 2004)).

370. *Id.* para. 50 (quoting *Vasiljević*, Case No. IT-98-32-A, para. 287).

371. Prosecutor v. Furundžija, Case No. IT-95-17/1-T, Judgement, para. 246 (Int'l Crim. Trib. for the Former Yugoslavia Dec. 10, 1998).

372. 2 INT'L COMM'N OF JURISTS, CORPORATE COMPLICITY & LEGAL ACCOUNTABILITY 21 (2008).

of the corporation in the context of its business relations, as was allegedly the case in *Talisman*[373] and *Kiobel*.[374]

To summarize the main findings of this Article, the line between merely doing business with a bad actor and acts that give rise to complicity liability is crossed when a corporate activity, whether or not of a routine commercial nature, has a substantial effect on the commission of human rights violations, and the corporation had the relevant knowledge. Clearly, the application of such a test in practice, and how to clarify its criteria, depends on context. However, clarity about the broad features of the test to be applied in order to determine the objective and mental elements of corporate complicity liability is an important step towards setting the framework that should guide the future debate on corporate complicity liability and corporate due diligence responsibilities. Just as important is to challenge recent trends in the influential ATS jurisprudence that are based on mistaken assumptions and should not serve as a model for future developments.

373. Presbyterian Church of Sudan v. Talisman Energy, Inc., 582 F.3d 244, 262 (2d Cir. 2009).

374. Kiobel v. Royal Dutch Petroleum Co., 621 F.3d 111, 193 (2d Cir. 2010) (Leval, J., concurring in the judgment).

Not Only 'Context': Why Transitional Justice Programs Can No Longer Ignore Violations of Economic and Social Rights

SAM SZOKE-BURKE*

SUMMARY

* LL.M., New York University School of Law; B.A., LL.B. (Hons), Monash University, Australia; Legal Researcher, Columbia Center on Sustainable Investment. All views expressed in this Article are the author's and do not necessarily reflect the views of the Columbia Center on Sustainable Investment. My sincere thanks to Paul van Zyl, Dr. Ioana Cismas, and Cristián Correa.

ABSTRACT

Transitional justice programs traditionally focused on breaches of civil and political rights and violations of bodily integrity, largely ignoring violations of economic and social rights (ESRs) and relegating socioeconomic issues to the category of 'background' or context. This approach is becoming increasingly untenable given that ESRs articulate binding and increasingly justiciable legal obligations. Considering past ESR violations can also provide crucial insight into the causes of past conflict, and addressing socioeconomic grievances can help to reduce the chances of future rights violations or civil unrest. This Article sets out when transitional justice ought concern itself with breaches of ESRs using the 'respect, protect, fulfill' framework of state obligations. Drawing on past examples, the Article argues that failures to respect and protect ESRs are usually discrete enough to be included in the mandates of truth commissions, reparations schemes, and, in some cases, criminal prosecutions. Decentralization programs and the vetting of corrupt economic actors can also effectively address past ESR violations and lead to socioeconomic improvements. Addressing state failures to fulfill ESRs is a more complicated question, although there are occasions where such violations should be included in transitional justice mandates. Ultimately, transitional justice can no longer ignore that ESRs articulate non-negotiable and clearly defined standards, which often hold the key to stable and sustainable political transitions.

INTRODUCTION

The field of transitional justice traditionally focused on breaches of civil and political rights when seeking to respond to periods of conflict, systemic rights violations, and political transition. Early instantiations of transitional justice generally ignored violations of economic and social rights (ESRs) or relegated them to issues of "background" or context.[1] While some transitional justice mechanisms may not be well suited to effectively respond to ESR violations, to completely exclude ESRs from transitional justice programs is imprudent. Socioeconomic grievances often figure as an important element to the dynamics of past conflict or atrocity and thus need to be investigated and understood. Properly addressing ESR

1. *See, e.g.*, Dustin N. Sharp, *Addressing Economic Violence in Times of Transition: Toward a Positive-Peace Paradigm for Transitional Justice*, 35 FORDHAM INT'L L.J. 780, 781–83 (2012) [hereinafter Sharp, *Addressing*] (noting that transitional justice has historically treated economic violations as "little more than useful context").

violations can also help to prevent recurrence of rights violations or conflict. Further, ESRs are now justiciable in many forums.[2] The reasons for, and instances of, the inclusion of ESRs in transitional justice programs are detailed in Part I. Despite these considerations, many commentators advocate for exercising caution when considering whether to include ESRs within transitional justice mandates, arguing that addressing ESRs can lead a project into the realms of development, which requires tools and strategies that differ from those employed in transitional justice.[3] Part II explores these arguments. It then seeks to refute those concerns by exposing erroneous assumptions regarding civil and political rights as compared with ESRs, by debunking misplaced assumptions about how ESRs can and cannot be productively incorporated into transitional justice mandates, and by addressing certain practical considerations that can facilitate such incorporation.

In Part III the Article sets out when transitional justice ought to concern itself with breaches of ESRs using the 'respect, protect, fulfill' framework of state obligations and by considering past examples. State failures to respect and protect ESRs are generally discrete enough to be effectively included in transitional justice mandates. For instance, truth commission mandates now often include economic crimes or other forms of socioeconomic injustice,[4] and international criminal courts have used the crimes of enslavement, persecution, and genocide to prosecute crimes that include violations of ESRs.[5] Whether to include violations of the obligation to fulfill ESRs, which include notions of progressive achievement subject to a nation's "available resources,"[6] is a more complicated question. Nonetheless, various transitional justice mechanisms have the potential to meet failures to fulfill ESRs at the community level. Reparations schemes and decentralized governance have led to the better fulfillment of ESRs in traditionally marginalized communities,[7] and vetting processes can be used to root out corrupt public officials and to exclude complicit corporate actors from conducting business. Such efforts can strengthen economic governance and increase the amount of state revenue to be spent on health, education, welfare, and other ESRs.[8] Nationwide failures to fulfill ESRs will require extensive funding and sustained policy implementation and are therefore less suited to transitional justice responses. Nonetheless, the examples explored in this Article indicate how governments can capitalize on the opportunity presented by periods of

2. *See infra* notes 45–51 and accompanying text.

3. *See, e.g.*, Roger Duthie, *Transitional Justice, Development, and Economic Violence*, *in* JUSTICE AND ECONOMIC VIOLENCE IN TRANSITION 165, 172–73 (Dustin N. Sharp ed., 2014) (noting that the mechanics for achieving transitional justice differ from those used in development because "they are conceptually distinct initiatives that rest on separate grounds and relate to different dimensions of justice").

4. *See infra* Part III.A.

5. *See infra* Part III.C.

6. International Covenant on Economic, Social and Cultural Rights art. 2 para. 1, *opened for signature* Dec. 16, 1966, 993 U.N.T.S. 3 [hereinafter ICESCR] ("Each State Party to the present Covenant undertakes to take steps, individually and through international assistance and co-operation, especially economic and technical, to the maximum of its available resources, with a view to achieving progressively the full realization of the rights recognized in the present Covenant by all appropriate means, including particularly the adoption of legislative measures.").

7. *See infra* Part III.D–F.

8. *See infra* Part III.H.

transition to engrain ESRs into the fabric of a country's political culture and legal regime, which can positively impact on the future fulfillment of ESRs.

A. Cultural Rights?

This Article focuses on economic and social rights, rather than the usual grouping of economic, social, and cultural rights. However, this should not be regarded as denigrating the importance and indivisibility of cultural rights from other human rights. It is implicit in this Article's analysis that ESRs must be fulfilled through culturally specific and appropriate policies, and that cultural rights enshrined in instruments like the International Covenant on Economic, Social and Cultural Rights (ICESCR) are inviolable and indivisible. Indeed, the enforcement of the rights to culture and religion can lead to stronger and more secure socioeconomic entitlements, such as the articulation of indigenous or customary land rights.[9] This Article focuses on ESRs because these rights are most closely aligned to projects of development and are thus most often argued to be outside the bounds of transitional justice. It seeks to critique and clarify such arguments.

I. THE GRADUAL INCLUSION OF ECONOMIC AND SOCIAL RIGHTS

Transitional justice is concerned with achieving broad notions of justice, and maintaining peace and stability following a period of widespread human rights abuses and, usually,[10] a political transition.[11] Transitional justice mechanisms (truth commissions, prosecutions of human rights violations, reparations programs, vetting processes, memorials, and so on) tend to evaluate past wrongs against the standards and norms established by human rights and international humanitarian law.[12] Early instantiations of transitional justice focused on violations of civil and political rights

9. *See, e.g.*, U.N. Hum. Rts. Comm., Views: Communication No. 1457/2006, paras. 7.6–7.7, Commc'n 1457/2006, U.N. Doc. CCPR/C/95/D/1457/2006 (Apr. 24, 2009); Ctr. for Minority Rights Dev. v. Kenya, Commc'n 276/2003, (2009) A.H.R.L.R. 75, para. 209.

10. Compare, for example, Morocco's Equality and Reconciliation Commission, which was implemented by royal decree of King Mohammad IV in 2004 after five years on the throne. Dahir (Royal Decree) no. 1.04.42 10 of April 2004 approving Statutes of the Equity and Reconciliation Commission, *available at* http://www.ier.ma/article.php3?id_article=1395.

11. Ruti G. Teitel, *Transitional Justice Genealogy*, 16 HARV. HUM. RTS. J. 69, 69 (2003) ("Transitional justice can be defined as the conception of justice associated with periods of political change, characterized by legal responses to confront the wrongdoings of repressive predecessor regimes." (citation omitted)).

12. Naomi Roht-Arriaza, *The New Landscape of Transitional Justice*, *in* TRANSITIONAL JUSTICE IN THE TWENTY-FIRST CENTURY: BEYOND TRUTH VERSUS JUSTICE 1, 2 (Naomi Roht-Arriza & Javier Mariezcurrena eds., 2006) [hereinafter Roht-Arriaza, *The New Landscape*]; Evelyne Schmid & Aoife Nolan, *'Do No Harm'? Exploring the Scope of Economic and Social Rights in Transitional Justice*, 8 INT'L J. TRANSITIONAL JUST. 1, 3–4 (2014) (noting that the field of human rights, along with international criminal law and international humanitarian law, is the most frequently invoked normative framework invoked by transitional justice scholars and practitioners) (citing U.N. Secretary-General, *The Rule of Law and Transitional Justice in Conflict and Post-conflict Societies: Rep. of the Secretary-General*, para. 9, U.N. Doc. S/2004/616 (Aug. 23, 2004)).

at the expense of examining economic or social wrongs.[13] For instance, Argentina's National Commission on the Disappearance of Persons (known by its Spanish acronym, CONADEP) focused on disappearances, assassinations, and the treatment of those detained by the Argentine military.[14] The truth commissions of Chile (focusing on deaths, disappearances, and kidnappings),[15] El Salvador ("serious acts of violence"),[16] and Uruguay (enforced disappearances)[17] also gave most of their attention to violations of bodily integrity, leaving ESRs relatively unaddressed.[18] Similarly, the enabling legislation of South Africa's Truth and Reconciliation Commission limited the definition of "victim" to those who suffered gross human rights violations including killing, abduction, or torture, effectively relegating the structural economic violence of the apartheid system to be considered only as context.[19]

A. Understanding the Dynamics of Past Conflict and Atrocity

Many commentators recognize that focusing on violations of bodily integrity or political rights risks distorting understandings of the nature of past conflicts and violence.[20] While ideology, entrenched ethnic divisions, or other political grievances will often be a factor, many conflicts can count among their causes discontent regarding resource allocation or poor economic management, which directly impact socioeconomic rights.[21] For instance, the mass demonstrations that lead to large-scale

13. Sharp, *Addressing*, *supra* note 1, at 781–83; *see also* Zinaida Miller, *Effects of Invisibility: In Search of the 'Economic' in Transitional Justice*, 2 INT'L J. TRANSITIONAL JUST. 266, 267 (2008) ("The literature, institutions and international enterprise of transitional justice historically have failed to recognize the full importance of structural violence, inequality and economic (re)distribution to conflict, its resolution, transition itself and processes of truth or justice seeking and reconciliation." (citation omitted)).

14. *See generally* Emilio Crenzel, *Argentina's National Commission on the Disappearance of Persons: Contributions to Transitional Justice*, 2 INT'L J. TRANSITIONAL JUST. 173 (2008).

15. Law No. 355, Abril 25, 1990, para. 1, DIARIO OFICIAL [D.O.].

16. U.N. Comm'n on the Truth for El Salvador, From Madness to Hope: The 12-Year War in El Salvador, 11, U.N. Doc. S/25500 (1993).

17. Or "las desapariciones forzadas" in the original text. Resolución de la Presidencia de la República No. 858/200, pfo. 1, Diario Oficial [DO] No. 25.853, 9 de Agosto de 2000 (Uru.).

18. Dustin N. Sharp, *Interrogating the Peripheries: The Preoccupations of Fourth Generation Transitional Justice*, 26 HARV. HUM. RTS. J. 149, 169–70 (2013) [hereinafter Sharp, *Interrogating*].

19. Sharp, *Addressing*, *supra* note 1, at 793; Dustin N. Sharp, *Economic Violence in the Practice of African Truth Commissions and Beyond*, *in* JUSTICE AND ECONOMIC VIOLENCE IN TRANSITION, *supra* note 3, at 79, 86 [hereinafter Sharp, *Economic*]; Lars Waldorf, *Anticipating the Past: Transitional Justice and Socio-Economic Wrongs*, 21 SOC. & LEGAL STUD. 171, 175–76 (2012).

20. Miller, *supra* note 13, at 266; Sharp, *Addressing*, *supra* note 1, at 782–83; Sharp, *Interrogating*, *supra* note 18, at 170–71; Chandra Lekha Sriram, *Liberal Peacebuilding and Transitional Justice: What Place for Socioeconomic Concerns?*, *in* JUSTICE AND ECONOMIC VIOLENCE IN TRANSITION, *supra* note 3, at 27, 35; *cf.* Ruben Carranza, *Plunder and Pain: Should Transitional Justice Engage with Corruption and Economic Crimes?*, 2 INT'L J. TRANSITIONAL JUST. 310, 330 (2008) ("[T]he exclusion of corruption and economic crimes from transitional justice mechanisms does not necessarily mean that the role of these violations in abuse and conflict is being diminished. A popular view is that transitional justice is meant to address one part of the problem with the hope that it can contribute to the solution of the whole.").

21. *See, e.g.*, Naomi Roht-Arriaza, *Reparations and Economic, Social, and Cultural Rights*, *in* JUSTICE AND ECONOMIC VIOLENCE IN TRANSITION, *supra* note 3, at 109, 110 [hereinafter Roht-Arriaza, *Reparations*] ("The underlying causes of armed conflict tend to be structural and resource related as often

violence in Tunisia,[22] Egypt,[23] and Yemen[24] all had pressing socioeconomic concerns at their base, including poverty, unemployment, and corruption. Socioeconomic grievances also led to the 1932 massacre in El Salvador of over 30,000 peasants and farm-laborers: The victims had sought to revolt because of concerns regarding land distribution and stark socioeconomic inequality.[25]

Rule by dictatorial or rights-violating regimes will also often lead to widespread economic and social deficiencies and stark societal inequality,[26] or may even involve positive breaches of social and economic rights. For instance, education can be co-opted by the government and used as a propaganda tool, and populations can be forcibly displaced or subjected to famine.[27] Thus, ESR violations can be as devastating on populations as violations of bodily integrity[28] or other civil and political rights—indeed, the division between these two characterizations of right violations becomes harder to discern in instances of forcible displacement and the use of mass starvation, given the physical impacts on victims that inevitably result. Consideration of such factors merely as background or context reinforces the myth that socioeconomic issues will be resolved over time,[29] or with the advent of democracy;[30] it also obfuscates the direct and immediate obligations that arise from state duties to respect, protect, and fulfill ESRs.

B. Preventing Recurrence and Fostering Stable Transitions

Ignoring ESRs does not only distort historical narratives: It also risks leaving certain causes of past violence unaddressed. This impedes the type of structural or

---

as ideological."); *cf.* Waldorf, *supra* note 19, at 175 (challenging the assumption that economic and social rights (ESRs) can have a dominant role in causing conflict).

22. Eric Andrew-Gee, *Making Sense of Tunisia*, NEW REPUBLIC, Jan. 17, 2011, http://www.newrepublic.com/article/world/81611/making-sense-tunisia (describing the causes of the protests as corruption, unemployment, economic stagnation, and restrictions on freedom of the press).

23. Agence France-Presse, *Egypt Braces for Nationwide Protests*, HERALD, Jan. 25, 2011, http://www.herald.co.zw/egypt-braces-for-nationwide-protests/ (noting that the first day of protests that led to the sacking of President Mubarak was dubbed "the day of revolt against torture, poverty, corruption and unemployment" (internal quotation marks omitted)).

24. Malika Bilal, *Yemen: Bloody Protests and Broken Agreements*, AL JAZEERA (Dec. 27, 2011), http://www.aljazeera.com/indepth/spotlight/aljazeeratop102011/2011/12/2011122593511542382.html (describing protests "against government corruption, unemployment and woeful economic conditions").

25. Dermot Keogh, *El Salvador 1932: Peasant Revolt and Massacre*, 6 CRANE BAG, no. 2, 1982, at 7, 7.

26. Roht-Arriaza, *Reparations*, *supra* note 21, at 113.

27. Such breaches were recorded by Timor-Leste's commission. CHEGA! THE REPORT OF THE COMMISSION FOR RECEPTION, TRUTH, AND RECONCILIATION TIMOR-LESTE: EXECUTIVE SUMMARY 124, 125, 161 (2005) [hereinafter CAVR EXECUTIVE SUMMARY]. Another infamous example is the use of famine and starvation by Stalin in Soviet Ukraine in 1933. *See, e.g.*, TIMOTHY SNYDER, BLOODLANDS: EUROPE BETWEEN HITLER AND STALIN 24–25 (2010) .

28. *See, e.g.*, CAVR EXECUTIVE SUMMARY, *supra* note 27, at 44 (finding that of the 102,800 people who died under Indonesia's rule, 18,600 (18%) were killed while roughly 84,200 (82%) died because of hunger or illness, and noting that the number of deaths due to hunger and illness "exceed[s] the total that would be expected if the death rate due to hunger and illness had continued as it was in the pre-invasion peacetime period").

29. Miller, *supra* note 13, at 268.

30. *Id.* at 276.

systemic change required in a transitional context[31] and undermines the ability of governments and transitional justice programs to prevent recurrence of human rights violations. A failure to address systemic causes of, and the role of inequality in, conflict and systemic human rights abuses not only leaves open the possibility of renewed violence;[32] it may actively contribute to the precariousness of peace by reinforcing existing socioeconomic injustices, which can intensify social dissatisfaction.[33] Ignoring socioeconomic issues may also impede efforts to foster stable transitions. For instance, a recent report noted the national perception that the difficulties of Mali's transition out of civil war stem from a "lack of good governance, including in the sectors of justice, education, and health".[34] The International Crisis Group also recently emphasized that the fostering of a stable transition in the Central African Republic required the prioritization of "economic recovery and resource management."[35] At the same time, there may be limits to the ability of transitional justice to contend with widespread poverty and other issues of development. Exactly how transitional justice can grapple with issues of poverty and state failures to fulfill ESRs is considered in the following Subpart.

C. *The Increasing Justiciability of Breaches of Economic and Social Rights*

One explanation for the initial reluctance to consider ESRs by transitional justice institutions is tied to inherited biases and conceptions of hierarchies between different types of human rights.[36] These still exist despite authoritative characterizations of all human rights as "universal, indivisible and interdependent and interrelated."[37] This perceived hierarchy is based in part on the provision in the ICESCR for progressive achievement, to the maximum of a State's available resources, of the rights contained therein,[38] as opposed to the ostensibly more tangible responsibilities imposed by the International Covenant on Civil and Political

31. *See id.* at 280–81 ("The failure to include economic concerns in transitional justice mechanisms tends to make transition into a political rather than economic story, limiting knowledge of the economic underpinnings of conflict, narrowing the story of regime change and quelling discussion of development plans by quarantining them within the state and the executive rather than making them part of the transitional justice conversation.").

32. *Id.* at 287–90; *see also* Sharp, *Addressing*, *supra* note 1, at 783 (arguing that "'never again' has little meaning if the self-imposed blind spots of the field distort our understanding of the conflict").

33. *See* Miller, *supra* note 13, at 286 (arguing that a reparations scheme that is employed without a deep consideration of the underlying economic drivers of conflict will not lead to structural change or resolution of the fundamental origins of the conflict).

34. VIRGINIE LADISCH, INT'L CTR. FOR TRANSITIONAL JUSTICE, POSSIBILITIES AND CHALLENGES FOR TRANSITIONAL JUSTICE IN MALI 4 (2014), *available at* https://www.ictj.org/sites/default/files/ICTJ-Briefing-Mali-Assessment-2014.pdf.

35. Int'l Crisis Grp., *Central African Republic: A Transition at Risk*, INT'L CRISIS GRP. BLOG (Oct. 7, 2014), http://blog.crisisgroup.org/africa/2014/10/07/central-african-republic-a-transition-at-risk.

36. Sharp, *Addressing*, *supra* note 1, at 796; *see also* Waldorf, *supra* note 19, at 173 ("[T]ransitional justice has been heavily influenced by human rights and, as such, has replicated that discpline's longstanding legalistic bias towards civil and political rights . . . ."); *cf.* Schmid & Nolan, *supra* note 12, at 2–3 (responding to and critiquing traditional views of transitional justice, which tend to minimize the import of economic and social rights).

37. World Conference on Human Rights, June 14–25, 1993, *Vienna Declaration and Programme of Action*, para. 5, U.N. Doc. A/CONF.157/23 (July 12, 1993) [hereinafter *Vienna Declaration*].

38. ICESCR, *supra* note 6, art. 2, para. 1.

Rights.[39] However, the ICESCR still creates obligations for States. Specifically, the duty to "take steps" is an immediate and concrete obligation.[40] In addition, States parties have duties to respect, protect, and fulfill economic, social, and cultural rights (ESCRs).[41] The obligation to respect prohibits state interference with individuals' exercise or enjoyment of ESCRs.[42] The obligation to protect requires States to prevent third parties from violating those rights.[43] The obligation to fulfill requires States to take appropriate steps toward the full realization of ESCRs, which includes obligations for both immediate and progressive action.[44]

ESR obligations are also increasingly justiciable: They are enshrined in some States' constitutions,[45] or constitutional jurisprudence,[46] as well as in some regional human rights regimes.[47] In addition, the recent Optional Protocol to the ICESCR creates a process for individual communications to the Committee on Economic, Social and Cultural Rights.[48] There exist many other international instruments in which ESCRs are enshrined,[49] as well as the provision for similar rights under customary international law[50] and international humanitarian law.[51] The increasing

39. *See* International Covenant on Civil and Political Rights art. 2, Dec. 19, 1966, S. TREATY DOC. NO. 95-20, 999 U.N.T.S. 172 [hereinafter ICCPR] (requiring that each State Party to the Covenant protect the rights provided for by the Covenant and undertake measures to ensure their protection).

40. Comm. on Econ., Soc. & Cultural Rights, Rep. on its 5th Sess., Nov. 26–Dec. 14, 1990, annex 3, at 83, U.N. Doc. E/1991/23 (1991) ("[W]hile the full realization of the relevant rights may be achieved progressively, steps towards that goal must be taken within a reasonably short time after the Covenant's entry into force for the States concerned. Such steps should be deliberate, concrete and targeted as clearly as possible towards meeting the obligations recognized in the Covenant.").

41. Comm. on Econ., Soc. & Cultural Rights, Rep. on its 24th Sess., Nov. 13–Dec. 1, 2000, U.N. Doc. E/C.12/2000/13 (Oct. 2, 2000) ("Like civil and political rights, economic, social and cultural rights impose three different types of obligations on States: the obligations to respect, protect and fulfill. Failure to perform any one of these three obligations constitutes a violation of such rights.").

42. *Id.*

43. *Id.*

44. *See* Schmid & Nolan, *supra* note 12, at 6 (outlining examples and methods that States can use to realize their obligations).

45. *See, e.g.*, CONSTITUTION, art. 43 (2010) (Kenya) (right to health, adequate housing, food, water, social security, and education); CONSTITUTION OF THE REPUBLIC OF NAMIBIA, art. 20 (right to education); S. AFR. CONST., 1996, arts. 22 (freedom of trade, occupation, and profession), 26 (right to adequate housing), 27 (right to health care, food, water, and social security), 29 (right to education).

46. *See, e.g.*, Narayan v. Bihar, A.I.R. 1989 S.C. 348, 354–55 (India) (implying right to health from right to life); Tellis v. Bombay Mun. Corp., A.I.R. 1986 S.C. 180, 189–90 (India) (implying right to "livelihood" and, effectively, adequate shelter from the right to life).

47. *See* African Charter on Human and Peoples' Rights, *opened for signature* June 27, 1981, O.A.U. Doc. CAB/LEG/67/3 rev. 5, arts. 14 (right to property), 15 (right to work), 16 (right to health), 17 (right to education), 21 (right to free disposal of wealth and natural resources); Association of South East Asian Nations [ASEAN], *ASEAN Human Rights Declaration*, 21st Summit (Nov. 19, 2012), arts. 27 (right to work), 28 (right to adequate standard of living), 29 (right to health), 30 (right to social security), 31 (right to education).

48. Optional Protocol to the International Covenant on Econ., Soc. and Cultural Rights, G.A. Res. 63/117, art. 2, U.N. Doc. A/RES/63/117 (Dec. 10, 2008) (effective May 2013).

49. *See* Sharp, *Addressing*, *supra* note 1, at 795 n.49 (citing various intergovernmental documents incorporating economic, social, and cultural rights (ESCRs)).

50. U.N. Comm. on Econ., Soc. & Cultural Rts., Consideration of Reports Submitted by States Parties under Articles 16 and 17 of the Covenant, para. 12, U.N. Doc. E/C.12/1/Add.69 (Aug. 31, 2001).

51. *Id.*; *see* Duthie, *supra* note 3, at 185 ("[U]nlawful interference with people's health, housing, food, water, or education, [] can constitute the crimes of willful killing, unlawful deportation or transfer,

number of forums in which individuals can bring claims related to breaches of their ESRs clearly indicates one way in which such rights can be addressed by transitional justice programs. Given this development, and the concreteness of obligations created by instruments like the ICESCR, it becomes less tenable to argue that including ESRs in transitional justice mechanisms is unrealistic or implausible. Other arguments against incorporating ESRs in transitional programs are addressed in Part II, below. Before considering such arguments, the Article, in the following Subpart, explores the complexity of determining which types of ESR violations would be most appropriately included within mandates of transitional justice processes.

D. Determining Which Types of Economic and Social Rights Must Be Included

Transitional justice mechanisms can no longer turn a blind eye to the violation of ESRs. To do so not only perpetuates anachronistic conceptions of ESRs as lower on the hierarchy of rights, it also distorts findings and misaligns policies, which has implications for the right to truth and for efforts to avoid recurrence of violence. To downgrade or ignore ESRs is to fail to capitalize on the unique opportunity that periods of transition present for reinvention and reform of a State's legal culture and rule of law; rejecting the prospect of strengthening a population's ESRs may also taint the legitimacy of the State's juridical culture. Indeed, as discussed below, truth commissions are increasingly considering issues of socioeconomic injustice.[52] At the same time, transitional justice mechanisms, or the government entities creating them, will need to prioritize which types of ESR violations will be focused on. Some issues related to ESRs may require sustained and long-term attention and policy to be properly understood and addressed, and may thus not be suited to intensive attention by transitional justice mechanisms. Others will be sufficiently discrete and remediable to be effectively addressed by a transitional justice program. It will often thus be appropriate for such mechanisms to be given broad mandates, within which they can determine specific priorities and areas of focus.

More precise delineations as to what should fall within, and outside of, transitional justice mandates will depend on the specific context, including the nature of past rights violations, and the resource constraints of the institution.[53] As Dustin Sharp has pithily observed, "[T]here are no easy answers, only trade-offs that must be carefully analyzed."[54] What can realistically be considered as fodder for a truth commission or other transitional justice process thus merits discussion. In the following Part, this Article considers arguments concerning the limitations or incapacities of transitional justice in dealing with ESRs. In Part III, it goes on to explore examples of transitional justice mechanisms that effectively identified and responded to ESR violations, or that have had the effect of better fulfilling ESRs.

---

collective punishment, pillage, destruction of property, attacking cultural property, or starvation . . . .").

52. *See infra* Part III.A.

53. *See, e.g.*, Sharp, *Economic*, *supra* note 19, at 106 (noting that "while the work of some truth commissions is starting to broaden, it is not clear that the budgets and time allocated . . . have increased commensurately").

54. Dustin N. Sharp, *Conclusion: From Periphery to Foreground*, *in* JUSTICE AND ECONOMIC VIOLENCE IN TRANSITION, *supra* note 3, at 289, 294.

II. LIMITATIONS OF INCLUDING ECONOMIC AND SOCIAL RIGHTS

A. *The Wrong Tools*

The most convincing reasons advanced for limiting consideration of ESRs by transitional justice mechanisms tend to focus on tactics and efficacy—on transitional justice's ability to foster any amount of meaningful socioeconomic change—rather than on arguments of principle or doctrinal coherence. The first argument concerns development, rather than specifically addressing breaches of ESRs, but is nonetheless relevant given that populations in need of development assistance are usually beset by violations of ESRs.[55] Societies emerging from authoritarianism or conflict are often affected by poverty, damaged infrastructure, and low levels of governance and social capital.[56] Such problems can be characterized as within the bounds of the project of development, rather than of transitional justice. Transitional justice and development will interact in many different ways, but ultimately, so the argument goes, the tools of transitional justice are not suited to addressing developmental shortcomings.[57] The pursuit of economic development (characterized by economic growth distribution)[58] or human development (defined as the enlargement of people's choices)[59] are both long-term projects, requiring decades of applied policy consideration. Transitional justice in a given country, on the other hand, tends to have a relatively short lifespan.[60] Truth commissions, for instance, generally have one shot at making recommendations for systemic reforms, and they cannot revise their recommendations for socioeconomic policies as conditions on the ground change.[61] Many transitional justice mechanisms also require a certain level of development to operate.[62] Transitional justice may thus struggle to achieve long-lasting socioeconomic development, which weakens the utility of including state failures to fulfill ESRs within transitional justice mandates.

---

55. Pablo de Greiff, *Articulating the Links between Transitional Justice and Development: Justice and Social Integration*, *in* TRANSITIONAL JUSTICE AND DEVELOPMENT: MAKING CONNECTIONS 28, 29 (Pablo de Greiff & Roger Duthie eds., 2009) ("[A] good number of transitional societies face immense development challenges, and a good number of developing countries face abiding 'justice deficits' concerning massive human rights abuses in their pasts.").

56. *Id.* at 29–30.

57. *See id.* at 30–31 (addressing some issues regarding developmental problems in transitional regimes); *see also* Duthie, *supra* note 3, at 201 ("[Traditional justice] measures are facing different kinds of political, legal, and practical challenges and constraints; measures that were initially designed to deal with a narrow set of civil and political rights violations cannot necessarily deal as effectively with economic and social rights violations without being adapted, without changes in international and national law, and without a minimum level of coherence with broader development interventions.").

58. de Greiff, *supra* note 55, at 33–34.

59. *Id.* at 49 (quoting U.N. DEV. PROGRAMME, HUMAN DEVELOPMENT REPORT 1990, at 1 (1990)).

60. Waldorf, *supra* note 19, at 179; *see also* Schmid & Nolan, *supra* note 12, at 19 (discussing another scholar's view that "transitional justice is inherently concerned with . . . short-term change," among other factors).

61. *See* Waldorf, *supra* note 19, at 176–77.

62. *Id.* at 30–31 ("[T]rials require operative courts; reparations programs require, among other things, resources to distribute; even the mildest form of institutional reform, vetting, requires institutions strong enough to withstand having personnel removed.").

B. *Insufficient Resources*

A second argument concerns the fact that transitional justice usually operates in contexts where state resources are severely limited.[63] Transitional justice mechanisms are stretched to their limits even without considering breaches of ESRs, the investigation of which may require different skills and expertise. Expanding the mandate to include ESRs without a corresponding increase in funding thus risks overburdening transitional justice,[64] diluting its efficacy. For instance, truth commission findings risk being less concrete, their analysis overly general, and their recommendations "utopian" and without distinct mechanisms for achieving the desired results.[65] Studies have also shown that in jurisdictions where economic crimes can be prosecuted, authorities still tend to prioritize the prosecution of more traditional crimes.[66] The gist of this argument, then, is not that transitional justice is necessarily unable to have a practical effect on questions of inequality and development, but that if it were to attempt to do so, it would risk neglecting more conventional transitional justice endeavors, such as deterring future atrocities and upholding the dignity of victims of physical or sexual violence.

This argument has even more force where beneficiaries of past socioeconomic injustice remain in positions of power: In seeking to protect their economic interests, they may obstruct or undermine transitional justice processes aimed at altering the status quo.[67] The following Subpart responds to the arguments discussed in Subparts A and B, providing reasons why they should not lead to the complete exclusion of ESRs within transitional justice programs.

C. *Responses to 'Limitation' Arguments*

The arguments raised in Subparts A and B above do not provide a sufficient foundation for the per se freezing out of ESRs from transitional justice. Several issues, in addition to the above discussion of the binding nature of state obligations with regards to ESRs, need to be considered. First, breaches of the obligation to respect and protect ESRs will not usually be so aspirational or long-term as to be unresponsive to transitional justice mechanisms. For instance, forced displacement (violating the right to an adequate standard of living and housing, among others)[68] can be the subject of truth finding and recommendations; victims can also seek restitution or compensation, and those responsible can be prosecuted or otherwise held to account.[69]

---

63. *Id.* at 40.

64. *Id.*; Sharp, *Interrogating*, *supra* note 18, at 173.

65. de Greiff, *supra* note 55, at 40.

66. *E.g.*, Duthie, *supra* note 3, at 190–91.

67. de Greiff, *supra* note 55, at 41; Duthie, *supra* note 3, at 189–90.

68. ICESCR, *supra* note 6, art. 11, para. 1.

69. FEDERICO ANDREU-GUZMÁN, INT'L CTR. FOR TRANSITIONAL JUSTICE, CRIMINAL JUSTICE AND FORCED DISPLACEMENT: INTERNATIONAL AND NATIONAL PERSPECTIVES (2013), https://www.ictj.org/sites/default/files/ICTJ-Research-Brief-Displacement-Criminal-Justice-Andreu-Guzman.pdf ("Despite the absence of the crime of forced displacement from its statute, the International Criminal Tribunal for Rwanda (ICTR) addressed displacement through the crime against humanity of "inhuman acts," while the International Criminal Tribunal for the Former Yugoslavia's (ICTY) statute did include

Second, the project of remedying many civil and political rights violations will also often be a long-term or aspirational one,[70] yet this has not prevented such issues from being included in transitional justice mechanisms.[71] For instance, Timor–Leste's Commission for Reception, Truth and Reconciliation (known by its Portuguese acronym, CAVR) made recommendations regarding the improvements of the nation's courts, including ensuring sufficient numbers of judges and support staff,[72] which were aimed in part at ensuring the right to fair trial, a civil and political right.[73] Given Timor–Leste's severely decimated and under-trained judiciary around that time,[74] such a recommendation was as long-term and aspirational as any of CAVR's recommendations regarding ESRs. This undermines arguments that ESRs ought to be excluded from transitional justice projects because of their long-term or aspirational nature.

Third, while transitional justice measures require a baseline of development and resources to be effective,[75] countries that lack such resources at the time of transition ought not exclude having aims targeted at socioeconomic improvement. Governments can strategically sequence different processes aimed at remedying ESR violations so that they occur at a time where such redress or fulfillment is plausible. International financial or aid assistance can also be leveraged to increase a country's capacity to properly address ESR violations.

Fourth, concerns that including ESR violations will dilute the impact of a transitional justice mechanism do not necessarily mean that violations of ESRs should be excluded. This would undermine the notion of all human rights being "universal, indivisible and interdependent and interrelated."[76] Rather, such concerns indicate that considering all issues concerning civil and political rights and ESRs may not be possible and that determining which violations of which rights ought to be considered in detail by a transitional justice mechanism will thus depend on the particular context. The effects of breaches of ESRs can be as deleterious as breaches

---

deportation and the transfer of civilians as war crimes, and deportation as a crime against humanity.").

70. Schmid & Nolan, *supra* note 12, at 13 (giving the example of extra-judicial executions, which ought attract an immediate remedy as well as an aspiration to change the nation's law enforcement culture over time to ensure a more effective protection of the right to life).

71. *Id.* at 18.

72. CAVR EXECUTIVE SUMMARY, *supra* note 27, at 174–76.

73. ICCPR, *supra* note 39, art. 14(1) ("[E]veryone shall be entitled to a fair and public hearing by a competent, independent and impartial tribunal established by law.").

74. Shane Marshall, Justice, Fed. Court Austl., The East Timorese Judiciary: At the Threshold of Self-Sufficiency?, Address to the Conference of Supreme and Federal Court Judges at Darwin, Australia (Dec. 20, 2004), *available at* http://www.fedcourt.gov.au/publications/judges-speeches/justice-marshall/marshall-J-20041220 (discussing Timor-Leste's appointment of its first eight judges and two prosecutors in 2000); Shane Marshall, Justice, Fed. Court Austl., Update to The East Timorese Judiciary: At the Threshold of Self-Sufficiency?, Co-operating with Timor-Leste Conference at Victoria University in Melbourne, Australia (June 17, 2005), *available at* http://www.fedcourt.gov.au/publications/judges-speeches/justice-marshall/ marshall-j-20050617 (noting that in 2005 all twenty-two of Timor-Leste's judges, as well as all prosecutors and public defenders that were assessed, failed their examinations and evaluations and were thus suspended from duty).

75. *See* Marcus Lenzen, *Roads Less Traveled? Conceptual Pathways (and Stumbling Blocks) for Development and Transitional Justice*, *in* TRANSITIONAL JUSTICE AND DEVELOPMENT: MAKING CONNECTIONS, *supra* note 55, at 76, 103 n.13 (noting that "severe underdevelopment and resource scarcity put constraints on the implementation of transitional justice measures").

76. *Vienna Declaration*, *supra* note 37.

of civil and political rights, and deciding which rights should or should not be included requires nuance and careful attention, rather than an inflexible, binary approach.

Fifth, even if transitional justice is completely ill-equipped to solve a socioeconomic problem, that does not mean that failures to fulfill ESRs should be ignored: Their mere acknowledgement can re-articulate state obligations and ensure that such breaches cannot be merely explained away as a problem of insufficient resources.[77] Further, while such problems may be regarded as coming within the bounds of development, their articulation as human rights violations provides policy makers with guidance regarding what the law requires, based on international consensus and elaboration by human rights bodies and experts. Conceiving of individuals as rights holders, as opposed to beneficiaries of development programs, also reaffirms their dignity and agency, and empowers them to shape their own development and assert their rights.[78]

Finally, when targeting embedded patronage networks and other sources of corruption, the precariousness of peace must be taken into account.[79] Where vetting or prosecution of corrupt economic actors poses a significant risk of re-igniting conflict or campaigns of atrocity, the type of mechanism used to address ESR violations should be carefully considered. Reparations measures stand as the most likely candidate for an undisruptive and immediate response to past ESR violations, but future vetting or prosecution programs, or structural reforms, should not be ruled out. The incremental transitional justice advances, with the help of significant civil society activity, in Argentina and Morocco illustrate that measures regarded as risking destabilization at one point in time may become more plausible after the passing of time and the gradual change of power dynamics and governance structures.[80]

III. EFFECTIVE WAYS OF INCLUDING ECONOMIC AND SOCIAL RIGHTS WITHIN TRANSITIONAL JUSTICE MANDATES

A. Truth Finding

Truth commissions can play multiple roles with regard to violations of ESRs. First, the mandates of truth commissions often call for the scrutiny of systemic or

77. *See* Schmid & Nolan, *supra* note 12, at 18 (arguing that similar inabilities to fulfill civil and political rights, such as a failure to achieve sustainable rule of law reforms following a period in which extrajudicial executions were prevalent, do not mean that transitional justice is ill-equipped to consider those rights violations, and extending this logic to economic and social rights and socio-economic development).

78. Philip Alston, *The Two Words That Scare the World Bank*, WASH. POST, Nov. 7, 2014, http://www.washingtonpost.com/opinions/philip-alston-the-world-bank-treats-human-rights-as-unmentionable/2014/11/07/9091dafa-65da-11e4-9fdc-d43b053ecb4d_story.html ("[R]ights language recognizes the dignity and agency of all individuals and is intentionally empowering.").

79. Sam Szoke-Burke, *Searching for the Right to Truth: The Impact of International Human Rights Law on National Transitional Justice Policies*, 33 BERKELEY J. INT'L L. (forthcoming 2015) (on file with author).

80. *Id.*

structural causes of atrocity, which will naturally invite consideration of ESRs and socioeconomic conditions.[81] This also aligns with the right of victims and society in general to the truth about past human rights violations.[82] The right to truth has achieved *lex lata* with regard to "serious" human rights violations,[83] such as torture and disappearances, and should also extend, at least as a matter of *lex ferenda*, to knowing the truth of breaches of ESRs. Truth commissions are, then, in a good position to reveal the workings of socioeconomic injustice.

Thus far, the types of ESR violations considered by truth commissions generally fall within the duties to respect or protect such rights. CAVR fostered important revelations, using the terminology of ESRs,[84] regarding forced displacement and famine,[85] as well as the use of education for propaganda,[86] among others. Chad's commission did not characterize economic violence as breaches of economic rights, but it did uncover how the State routinely seized assets of political prisoners, passing them on to members of the State's secret police force (the DDS), regime loyalists, and even the DDS itself when funds ran low.[87] Sierra Leone's commission documented looting and extortion,[88] and Liberia's commission drew links between endemic corruption and the limitation or removal of educational and other socioeconomic opportunities, as well as considering land issues.[89]

Broader issues of development and social marginalization fitting within state failures to fulfill ESRs have also been included in truth commission findings. Timor–Leste's CAVR found that Indonesia's "overriding preoccupation with security," its "authoritarian style of government," and its "close collaboration with special interests," led it to breach its duty to fulfill ESRs.[90] Similarly, the Kenyan Truth,

---

81. de Greiff, *supra* note 55, 35–36.

82. *See, e.g.*, Velásquez-Rodríguez v. Honduras, Merits, Judgment, Inter-Am. Ct. H.R. (ser. C) No. 4, para. 177 (July 29, 1988) (noting that the State has an obligation to perform an "effective search for the truth"); El-Masri v. Former Yugoslav Republic of Maced., 2012-VI Eur. Ct. H.R. 263, 333 para. 191 (discussing the applicability of the right to truth).

83. Gonzales v. United States, Case 12.626, Inter-Am. Comm'n H.R., Report No. 80/11, OEA/Ser.L/V/II, doc. 69 para. 193 (2011) (holding that in the context of a repeated violation of the right to life, "[a] critical component of the right to access information is the right of the victim, her family members and society as a whole to be informed of all happenings related to a serious human rights violation").

84. CHEGA! THE REPORT OF THE COMMISSION FOR RECEPTION, TRUTH, AND RECONCILIATION TIMOR-LESTE, pt. 2, para. 130 [hereinafter CAVR REPORT] (explaining the difference between economic, social, and cultural rights in contrast with political and cultural rights).

85. *See id.* pt. 7.3, para. 3 ("Often displacement is in effect a form of arbitrary collective punishment, and as such is associated with violations of a range of human rights, civil and political as well as economic, social and cultural.").

86. *See id.* pt. 7.9, para. 122 ("In addition to the poor facilities and teaching, a fundamental problem with the education system under the Indonesians was what was taught. Rather than focusing on basic learning needs, the curriculum was explicitly oriented towards pro-Indonesian propaganda.").

87. Sharp, *Economic*, *supra* note 19, at 92–93 (citing the Commission d'Enquête du Ministère Chadien de la Justice and Les Crimes et Détournements de l'ex- Président Habré et de Ses Complices).

88. *Id.* at 96–97 (citing SIERRA LEONE TRUTH & RECONCILIATION COMM'N, 2 WITNESS TO TRUTH: REPORT OF THE SIERRA LEONE TRUTH & RECONCILIATION COMMISSION 35 (2004)).

89. *Id.* at 100 (quoting REPUBLIC OF LIBER. TRUTH & RECONCILIATION COMM'N, 2 CONSOLIDATED FINAL REPORT 16–17 (2009)).

90. CAVR EXECUTIVE SUMMARY, *supra* note 27, at 141 ("[T]he Commission has also found that the Indonesian State failed to realise the economic and social rights of the East Timorese people to the

Justice and Reconciliation Commission noted that ESRs created a duty to fulfill minimum core obligations, a duty which was "not only a normative but . . . also a practical standard."[91] While the Commission did not go on to expressly articulate breaches of the duty to fulfill, it found widespread instances of marginalization, whose indicators—public infrastructure, employment, education, health, housing, access to land, water, sanitation, and food security—overlapped with ESR standards.[92] The type of marginalization that communities experienced was found to vary, depending on the area: Provinces lacking natural resources received less government assistance, while those that had resources suffered government mismanagement[93] or exclusion from development projects.[94]

A second role that truth commissions can play is to characterize socioeconomic marginalization as violations of ESRs, in addition to constituting issues of development. This reframes the issue as one involving breaches of governmental obligations, the content of which has often already been considered and articulated by leading human rights jurists and experts.[95] Using rights language also provides civil society with a platform for advocacy,[96] and can protect public interest organizations from being delegitimized as subversive for seeking structural changes.[97] One commentator argues that the Guatemalan Commission on Historical Clarification's recommendations for progressive tax reform and increased spending on human development would have been more difficult for the government to ignore

---

maximum extent possible, and that at the end of the occupation, East Timor's development still lagged well behind that of even the poorest Indonesian provinces.").

91. TRUTH, JUSTICE AND RECONCILIATION COMM'N, KENYA, 2B REPORT OF THE TRUTH, JUSTICE AND RECONCILIATION COMMISSION para. 33 (2013) [hereinafter TJRC REPORT]. The Commission's mandate was to "establish an accurate, complete and historical record of violations and abuses of human and economic rights" and to "[i]nquire into and establish the reality of otherwise of perceived economic marginalisation of communities and make recommendations on how to address the marginalisation." *Id.* para 16. The Liberian Truth Commission was the only other commission at the time whose mandate included ESRs. *Id.* para. 18.

92. KENYA TRANSITIONAL JUSTICE NETWORK, SUMMARY: TRUTH, JUSTICE AND RECONCILIATION COMMISSION REPORT 14–15 (2013) [hereinafter KENYA SUMMARY], *available at* http://www.acordinternational.org/silo/files/kenya-tjrc-summary-report-aug-2013.pdf

93. TJRC REPORT, *supra* note 91, para. 8 (noting testimonies that described how the Central Province's fortunes "dwindled under the then President Moi"), para. 10 ("[A] sense of marginalisation exists even in regions regarded as relatively more endowed in resources than others."), para. 14 ("While Kajiado is perhaps rightly ranked as the richest county (based largely on asset-based assessment), its residents have some of the lowest levels of access to social goods such as education, health, water and sanitation and physical infrastructure such as roads and can rightly claim marginalisation. In the Commission's view, however, this phenomenon seems to present a case of mismanagement of resources or outright corruption. Resources that could improve the socio-economic condition of locals have either not been tapped, or have been diverted to other extraneous issues.").

94. KENYA SUMMARY, *supra* note 92, at 14–15.

95. *See, e.g.*, Chris Albin-Lackey, *Corruption, Human Rights, and Activism: Useful Connections and Their Limits*, *in* JUSTICE AND ECONOMIC VIOLENCE IN TRANSITION, *supra* note 3, at 139, 140–41 (distinguishing "positive" governmental human rights obligations from "negative" obligations).

96. *Cf.* Sharp, *Addressing*, *supra* note 1, at 803 ("[I]f framed properly, [. . .] recommendations [addressing socioeconomic inequalities] might nevertheless serve as a strong lobbying platform for civil society actors who wish to press for reforms.").

97. *Cf.* Lisa J. Laplante, *Transitional Justice and Peace Building: Diagnosing and Addressing the Socioeconomic Roots of Violence through a Human Rights Framework*, 2 INT'L J. TRANSITIONAL JUST. 331, 351 (2008) (arguing that truth commissions enable people to advocate for structural change with less fear of prosecution).

if they were framed as rights violations.[98] It must be noted that while using rights language is certainly not detrimental to the prospects that reforms will be adopted, truth commission articulation of ESR violations is unlikely to be the silver bullet that motivates governmental action. Even truth commission recommendations regarding civil and political rights are often not implemented.[99] Political will is the necessary ingredient, and using the language of rights and violations can help to catalyze civil society as well as increasing pressure on, and shifting the will of, those exercising political power.

A third function of truth commissions is to make recommendations for reform to prevent or minimize recurrence of ESRs violations. Such recommendations are more likely to be effective when based on the sort of deep understanding of past events that commissions can possess after months or years of public inquiry. While understanding past violations is not in itself sufficient to be able to prevent recurrence,[100] it is an important starting point. Truth commissions cannot offer sustained monitoring and adjustment of socioeconomic policies necessary for long-term development,[101] but when they are staffed by appropriately qualified commissioners, they can set into action mechanisms that increase the chances that policies and programs will address ESRs. Thus, truth commission recommendations can address failures to respect and protect ESRs, and can sometimes also set into motion government programs and policies to address failures to fulfill them, such as reforms designed to decentralize government decision-making or facilitate participatory budgeting by communities. Having established that truth commissions can indeed play an important role with regard to violations of ESRs, this Article, in the next Subpart, considers what this might look like in practice; specifically, it explores the question of whether a separate commission would be best placed to consider violations of ESRs, or whether it would be preferable to have a single truth commission that manages a mandate including civil and political, as well as economic and social, rights.

B. A Separate Commission Focusing on Economic and Social Rights?

The U.N. Office of the High Commissioner for Human Rights has noted that consideration of ESRs requires a different set of skills and expertise than those needed to properly address traditional grave breaches of human rights.[102] Given the potential concerns of diluting a truth commission's mandate, or the over-stretching of its resources, one alternative is for the investigation of ESRs to be undertaken by a separate body, such as a marginalization and social justice commission or a separate arm of a truth commission, which possesses the necessary technical expertise to appropriately respond to such violations. Because ESRs demand a different skill set,

98. *Id.* at 350–51.

99. *See, e.g.*, Duthie, *supra* note 3, at 196–97 (discussing numerous instances where truth commission recommendations concerning various rights were ignored).

100. *Cf.* de Greiff, *supra* note 55, at 36 ("[U]nderstanding the dynamics leading to violations may be a necessary but not a sufficient condition for changing those dynamics . . . .").

101. *See supra* Part II.A.

102. Office of the U.N. High Comm'r for Hum. Rts., *Rule-of-Law Tools for Post-conflict States*, 9, U.N. Doc. HR/PUB/06/1 (2006).

a more technocratic body might be best suited to understanding past causes of economic and social injustice. It may also be able to develop sophisticated policies, such as tax concessions or other complex financial arrangements that better leverage a State's available resources to provide redress for violations of ESRs, including failures to fulfill them.

Various countries have created commissions to deal with the challenges posed by widespread poverty. However these have generally been outside of the transitional justice context, and are usually not staffed by development economists or other independent experts on socioeconomic policy. For example, Illinois's Commission on the Elimination of Poverty was made up of local and state public representatives, and members of civil society organizations concerned with homelessness, poverty, health, and food security.[103] In contrast, the Commissioners of Scotland's Poverty Truth Commission include individuals who have experienced poverty in their own lives as well as government and civil society representatives with experience in policy issues including employment and poverty.[104] Lastly, the National Anti-poverty Commission of the Philippines is staffed by the heads of government agencies and representatives from different stakeholder groups, including farmers, indigenous people, women, and non-government organizations and is of a different nature.[105] It has existed for more than ten years, and evaluates and monitors the government's anti-poverty program development and funding.[106] These government-backed bodies can be contrasted with more temporary, civil society-generated poverty truth commissions in the United States, that seek to catalyze government action on poverty.[107]

The prospect of having a separate, more ESRs-focused commission presents a dilemma: On the one hand, such expertise is needed to make the most of the scarce resources available for transitional justice; on the other hand, those resources would be consumed more quickly if two bodies, each with their own set of staff and processes, operated in tandem. Implementing a separate poverty commission would involve serious tradeoffs, including limiting the extent to which the truth regarding civil and political rights can be pursued. Having a separate commission for ESRs could also reinforce anachronistic human rights hierarchies and perpetuate the myth

---

103. *Commission Members*, COMM'N ON THE ELIMINATION OF POVERTY, http://www.illinois.gov/poverty/Pages/members.aspx (last visited June 15, 2015).

104. *The Poverty Truth Commission: Commissioners*, FAITH COMMUNITY SCOT., http://www.faithincommunityscotland.org/poverty-truth-commission/commissioners/ (last visited June 15, 2015) ("[Our commissioners] include the Scottish Government, Glasgow City Council, faith communities, students and school leavers, community activists, people involved in the criminal justice system, representatives of political parties, academics, refugees, advice services, business leaders, carers and volunteers.").

105. Letter from President of the Philippines to Secretary Jose Eliseo M. Rocamora, Nat'l Anti-Poverty Comm'n (Jan. 9, 2012), *available at* http://maps.napc.gov.ph/drupal/sites/default/files/documents/NAPC_SR_Appointment.pdf.

106. *Service Charter*, NAT'L ANTI-POVERTY COMM'N, http://maps.napc.gov.ph/drupal/about/servicecharter (last visited June 15, 2015).

107. *See, e.g.*, JAMES EDWARD BEITLER III, REMAKING TRANSITIONAL JUSTICE IN THE UNITED STATES: THE RHETORICAL AUTHORIZATION OF THE GREENSBORO TRUTH AND RECONCILIATION COMMISSION 137 (2013) (noting that the Poor People's Economic Human Rights Campaign held a three-day commission in Cleveland, Ohio in 2006, and its commissioners included international and domestic commissioners, while the Union Theological Seminary's Poverty Truth Commissions had been staffed mainly by religious figures).

of economic and social rights as being of secondary importance. For this reason, including both sets of rights within the mandate of a truth commission, or having a separate but related 'arm' of a commission that is charged with making recommendations regarding prevention of ESR violations, is preferable to having a distinct commission.

A separate commission would also require detailed policies regarding how it would interact with its counterpart, civil-and-political-rights-focused commission to avoid institutional conflict. Sierra Leone[108] and Peru[109] each experienced institutional difficulties between their truth commissions and courts, including conflicts as to which institution's proceedings should take priority and failures of one institution to pursue investigations referred to it by the other. The operation of two commissions may be easier to manage than the interface between a truth commission and a court because there will be less divergence in processes. Nonetheless, it is foreseeable that some of the institutional difficulties that occurred in Sierra Leone and Peru could occur in such a setting. This is not fatal to the idea of having two separate commissions, but rather requires a careful approach to policy and procedure. Incorporating a poverty commission as a separate arm of the commission could potentially reduce (but not eliminate) the potential for institutional conflict by limiting the barriers between the different truth finding endeavors. It might also reduce duplicated expenditures by combining resources and sharing facilities and support staff. In addition, there will be more opportunities to share institutional knowledge, including being privy to testimony from both arms of the commission.

Given that transitional justice contexts will usually be plagued by resource shortages, and that additional mechanisms tend to bring added institutional complexity and potential for conflict, a separate commission for ESRs will not always be a plausible option. The efforts of truth commissions in Timor–Leste and Kenya also indicate that properly staffed commissions can productively address both sets of rights. A more cost-effective way of including technical socioeconomic solutions to resource shortages may be to encourage the appearance of expert witnesses at truth commission proceedings, or to employ consultants to assist with the design of economic or budgetary recommendations and mechanisms, and with other areas outside the expertise of commission members.

C. Litigation

Breaches of the duty to respect and protect ESRs, including large-scale violations, have been litigated in varying jurisdictions. The Inter-American Court of Human Rights in *Ituango Massacres v. Colombia*[110] found instances of forced labor[111]

---

108. *See generally* Ari Bassin & Paul van Zyl, *The Story of* Samuel Hinga Norman *in Sierra Leone: Can Truth Commissions and Criminal Prosecutions Coexist after Conflict?*, *in* HUMAN RIGHTS ADVOCACY STORIES 229 (Deena R. Hurwitz et al. eds., 2009).

109. *E.g.*, Eduardo González Cueva, *The Peruvian Truth and Reconciliation Commission and the Challenge of Impunity*, *in* TRANSITIONAL JUSTICE IN THE TWENTY-FIRST CENTURY: BEYOND TRUTH VERSUS JUSTICE, *supra* note 12, at 70, 83–85 (discussing the processes of truth commissions in transitional justice cases).

110. Preliminary Objections, Merits, Reparations, and Costs, Judgment, Inter-Am. Ct. H.R. (ser. C) No. 148 (July 1, 2006).

and, in relation to forcible displacements, violation of the right to property.[112] Remedies granted included ordering the State to guarantee safe conditions for those who were forcibly displaced, to establish a housing plan for their benefit, to memorialize the violations, and to pay pecuniary and non-pecuniary compensation to named victims.[113] The inclusion of ESRs in state constitutions[114] provides another means of litigation, namely through domestic constitutional claims.

In addition, international criminal tribunals have successfully prosecuted conduct that violated ESRs, including the rights to work, to an adequate standard of living, and to health.[115] For example, in *Prosecutor v. Brđanin*, the International Criminal Tribunal for the Former Yugoslavia held that Bosnian Serb authorities persecuted Bosnian Muslims and Bosnian Croats by inflicting a series of socioeconomic deprivations on them. Specifically, the cumulative effect of the authorities' withholding of medical care and denial of the victims' rights to employment, freedom of movement, and proper judicial process "for the very reason of their ethnicity"[116] was held to constitute the international crime of persecution. Other tribunals have convicted defendants for the crime against humanity of enslavement[117] and have characterized "subjecting a group of people to a subsistence diet, systematic expulsion from homes and the reduction of essential medical services below minimum requirement", each of which violate ESRs, as "deliberate[ly] inflicting on the group conditions of life calculated to bring about its physical destruction, in whole or in part," thus constituting genocide.[118]

Litigation through international human rights bodies, national constitutional courts, and international criminal courts has an important role to play in stopping impunity and compelling States to compensate victim groups, especially for state failures to respect or protect those rights. Such cases have a remedial role for victims and, in theory, a deterrent role for future potential perpetrators. Addressing such issues on a structural level, however, including state failures to fulfill ESRs, will generally require policy shifts or truth commission recommendations for institutional and budgetary reform.[119] Another transitional justice tool that can remedy ESR

111. *Id.* para. 168.

112. *Id.* para. 183. The right to property, while not included in the ICESCR, has been described by the Independent Expert on the right of everyone to own property alone as well as in association with others as "enhancing both personal dignity and fostering socio-economic well-being, and is thus treated as an economic and social right for the purposes of this Article. Independent Expert, *The Right of Everyone to Own Property Alone as Well as in Association with Others*, Comm'n on Hum. Rts. para. 116, U.N. Doc. E/CN.4/1994/19 (Nov. 25, 1993) (by Luis Valencia Rodríguez).

113. *Ituango Massacres*, Inter-Am. Ct. H.R. (ser. C) No. 148, paras. 379, 390, 404, 407, 408.

114. *See supra* note 45 and accompanying text.

115. ICESCR, *supra* note 6, arts. 6, 11 and 12.

116. Case No. IT-99-36-T, Judgement, para. 1048 (Int'l Crim. Trib. for the Former Yugoslavia Sept. 1, 2004); *accord* OFFICE OF THE HIGH COMM'R FOR HUMAN RIGHTS, TRANSITIONAL JUSTICE AND ECONOMIC, SOCIAL AND CULTURAL RIGHTS, at 33–34, U.N. Doc. HR/PUB/13/5, U.N. Sales No. E.14.XIV.3 (2014) [hereinafter OHCHR].

117. *E.g.*, Prosecutor v. Sesay, Kallon & Gbao, Case No. SCSL-04-15-T, Judgement, paras. 2091, 2102, 2116 (Special Court for Sierra Leone Mar. 2, 2009).

118. Prosecutor v. Akayesu, Case No. ICTR-96-4-T, Judgement, para. 506 (Int'l Crim. Trib. for Rwanda Sept. 2, 1998); *accord* OHCHR, *supra* note 116, at 35–36.

119. *See* OHCHR, *supra* note 116, at 44–45 ("Institutional reform is a key dimension of transitional justice because it has the potential to trigger structural change. However, it is one of the most under

violations is the distribution of individual or collective reparations, which are considered respectively in the following Subparts.

D. Reparations

Reparations are an intuitive remedy for failures to respect or protect ESRs because they involve the transfer of goods, money, or other services to victims, which can directly impact on those victims' socioeconomic position.[120] They can also enhance the fulfillment of ESRs by improving access to public services. Reparations are thus a useful option for fulfilling the right of victims of ESRs violations to a remedy.[121] Reparations can include compensation or restitution of land, which can increase a recipient's economic capacity,[122] and scholarships or increased access to health services, which can remedy violations of the right to education or to health. Reparations for gross violations of civil and political rights usually include access to goods and services, which has the corollary of bolstering victims' ESRs and capacity for development.[123] Collective reparations, considered below, can also address these rights on a community level; large-scale reparations such as constructing or expanding hospitals, schools, or vital infrastructure can remedy violations of the rights to health, education, water, and so on. Reparations may also expose deficiencies that affect more than the immediate pool of victims, potentially acting as a catalyst for demands for improvement on a national scale.[124]

There are limitations to resorting to individual reparations as a means of remedying ESR violations. Firstly, including ESRs within the mandate of a reparations program, which will already be chronically under-resourced, will expand the pool of victims and thus further dilute the available remedies, minimizing their restorative potential.[125] The gravity of this limitation depends on the breadth of rights to be included and the number of persons affected. For instance, a victim whose land was illegally confiscated can have his or her right to property vindicated by restitution to the land or, where that is not possible, compensation. However, where the government has breached the right to health or education of a majority of the population by denying it adequate services (whether by failing to respect, protect, or fulfill those rights), there is little that a reparations scheme can do to remedy that violation for all. Reparations programs are generally too small[126] and are focused on discrete rights violations, rather than widespread inequality.[127]

---

researched and unexplored areas.").

120. de Greiff, *supra* note 55, at 37; Duthie, *supra* note 3, at 172.

121. *Cf.* Naomi Roht-Arriaza & Katharine Orlovsky, *A Complementary Relationship: Reparations and Development*, *in* TRANSITIONAL JUSTICE AND DEVELOPMENT: MAKING CONNECTIONS, *supra* note 55, at 170, 171 (discussing the reasons for and advantages of granting reparations in truth commissions).

122. *See, e.g.*, de Greiff, *supra* note 55, at 37 (noting that reparations that redistribute property rights can positively affect victims' socioeconomic well-being).

123. OHCHR, *supra* note 116, at 56.

124. *See, e.g.*, de Greiff, *supra* note 55, at 37–38 (noting that various truth commissions made recommendations that would have benefited more than just the direct victims of the previous regimes).

125. *Id.* at 40.

126. de Greiff, *supra* note 55, at 39.

127. Sriram, *supra* note 20, at 44.

A second limitation of employing reparations to address violations of ESRs is that they might distort perspectives of systemic problems that require government-administered, and -monitored, policies of economic redistribution or market reform. Reparations may interfere with a State's duty to fulfill ESRs by masking a continuing lack of redistribution, leaving more structural issues in the background and focusing on individual instances of socioeconomic harm.[128] Reparations programs aimed at individual victims may also conflict with, or crowd out discussion of, programs aimed at reducing poverty more generally,[129] potentially contributing to the continuation of inequality or marginalization of specific groups,[130] and denying the suffering of victims of those less tangible social or economic injustices.[131] While these risks are very real, they can generally be mitigated by reflective and strategic government policies and robust civil society engagement and advocacy. This is preferable to an either/or approach, given that ESRs and the right to remedy are both inviolable and indivisible.

While reparations are unlikely to foster macroeconomic development directly, they do have a useful role to play in rehabilitating victims. This in turn can enable "the (re)emergence of victims and survivors as actors with the initiative, motivation, and belief in the future that drive sustainable economic activity."[132] That reparations cannot cure poverty ought not mean that they have no role to play. Rather, this should inform exactly which socioeconomic issues are included within the bounds of reparation schemes. Thus, Peru's Truth and Reconciliation Commission aspired to adopt a broad approach to socioeconomic injustice but ultimately separated narrow violations (which it addressed) from broader concerns regarding nationwide poverty and social problems (which it did not).[133] It did, however, make recommendations for collective reparations for regions that had been marginalized and that suffered increased poverty as a result of the long period of violence.[134] The next Subpart explores how these types of collective reparations, along with strategic uses of decentralization and participatory budgeting, can be employed at a community or regional level to meaningfully address violations of ESRs, including failures to fulfill ESRs.

---

128. Miller, *supra* note 13, at 278, 280.

129. *See id.* at 284 (noting that reparations programs may redistribute power from autocratic to democratic institutions, but "[b]y definition" do not redistribute wealth to individuals).

130. Mariclaire Acosta & Esa Ennelin, *The "Mexican Solution" to Transitional Justice*, *in* TRANSITIONAL JUSTICE IN THE TWENTY-FIRST CENTURY: BEYOND TRUTH VERSUS JUSTICE, *supra* note 12, at 110–11 (giving an example of Mexico's lack of progress in punishing human rights abuses by the Mexican military regardless of the creation of a Special Prosecutor's Office to investigate these issues).

131. *See* Miller, *supra* note 13, at 285 (stating that granting aid to a limited class of perceived victims can increase "violence springing from resentment on the part of those not categorized as victims").

132. de Greiff, supra note 55, at 173.

133. Lisa Magarrell, *Reparations for Massive or Widespread Human Rights Violations: Sorting Out Claims for Reparations and the Struggle for Social Justice*, 22 WINDSOR Y.B. ACCESS JUST. 85, 95 (2003) ("[Peru's Comprehensive Reparation Plan (PIR)] cannot and should not be considered as one more instrument of social policy. The PIR does not seek to resolve problems of poverty, exclusion and inequality, which are structural in nature and respond to the overall operation of the political and economic system." (quoting COMISIÓN DE LA VERDAD Y RECONCILIACIÓN, INFORME FINAL para. 2.2.2.1 (2003), as translated by the author of that article)).

134. CRISTIÁN CORREA, REPARATIONS IN PERU: FROM RECOMMENDATIONS TO IMPLEMENTATION 5–7, (2013), *available at* http://www.ictj.org/sites/default/files/ICTJ_Report_Peru_Reparations_2013.pdf.

E. Collective Reparations

Collective reparations are forms of distribution of public goods or services that are designed for the benefit of all members of a region, group, or community, rather than for specific individual victims.[135] Collective reparations can address past ESR violations, and can be used to fulfill ESRs where recipient communities are in need of improvements in social or economic conditions. Whereas individual reparations seek to acknowledge harms to individual victims, collective reparations address collective harms and seek to restore social solidarity.[136] For instance, in Peru collective reparations were regarded as a key tool in addressing the historic marginalization of many rural and indigenous communities in the Andes and the Amazon, whose support networks, cultural identities, and local economies were broken down by years of systematic violence.[137]

Examples of collective reparations include allocation or restitution of land to communities for collective ownership and use, improvement of public services and infrastructure, restitution of religious or cultural sites, financial projects aimed at generating industry or commerce for victim groups, increased access to psychosocial support, exhumations of mass grave sites,[138] and memorials.[139] Additional collective reparations measures include decentralization or devolution of government decision-making and participatory budgeting programs, which are discussed in the following two Subparts of this Article. Such measures are especially attractive when the number of potential victims suffering breaches of economic or social rights is so large as to render the amount of money that would be payable as individual reparations so small as to be insignificant or even offensive to those receiving the reparation.[140] Collective reparations often constitute measures that the government is already duty-bound to provide: For instance, the Peruvian Truth Commission's Integral Reparations Program included recommendations to build a hospital,[141] which drew controversy by those arguing that the right to health demanded such measures regardless of the transitional justice context.[142] Nonetheless, collective reparations stand as one means of seeking to address past failures to fulfill ESRs in specific communities or regions.

---

135. Roht-Arriaza & Orlovsky, *supra* note 121, at 189–90.

136. *Id.* at 189.

137. CORREA, *supra* note 134, at 11.

138. Roht-Arriaza & Orlovsky, *supra* note 121, at 190.

139. Such as the special memorial constructed for traders in Ghana, who were brutalized, both physically and economically. Sharp, *Economic*, supra note 19, at 95 (citing GHANA NATIONAL RECONCILIATION COMM'N, 2 FINAL REPORT 42 (2005)).

140. *See* Duthie, *supra* note 3, at 191 (discussing the practical difficulties of providing pecuniary reparations in situations of widespread economic rights violations); *see also* Roht-Arriaza & Orlovsky, *supra* note 121, at 192 (identifying both the practical advantages and the benefits to individual victims of collective reparations).

141. COMISIÓN DE LA VERDAD Y RECONCILIACIÓN, INFORME FINAL para. 2.2.3.2 (2003).

142. CORREA, *supra* note 134, at 13; Laplante, *supra* note 97, at 352.

F. Decentralization

It is often the case that members of certain communities or regions experience greater marginalization and other socioeconomic wrongs than in other areas. In order to remedy this, such regions will require policy changes or interventions that are attuned to their needs. Where a government's services are provided by a centralized bureaucracy, usually based in the State's capital, the effects of past marginalization risk remaining unaddressed and even perpetuated. Truth commissions, civil society, and some post-transition governments have sought to remedy this problem by decentralizing decision-making—that is, giving increased control and authority to local government or community structures—for socioeconomic projects and policies.[143] Encouraging or mandating mechanisms for redistribution that decentralize decision-making can foster socioeconomic improvement and encourage the fulfillment of ESRs by enabling regions or communities to decide on which development projects and services are most needed without interference by the national government. More localized decision-making benefits from a more intimate knowledge of local conditions and needs, and can also empower local actors and community members.

The examples of Morocco and Peru show how effective decentralization can be in a transitional justice context. In Morocco, collective reparations were provided to eleven regions previously excluded from development programs.[144] Local councils determined how certain reparations funds would be spent, based on their constituents' priorities,[145] thus overcoming the past neglect of a centralized bureaucracy. A similar decentralization of collective reparations took place in Peru, where municipal bodies were given autonomy to determine how to use local and national government funding.[146] While some regions failed to benefit from the opportunity of shaping their own development programs, others consulted with local communities to determine budget priorities which better met local needs.[147] Providing reparations funding at the municipal level creates the potential for the decentralization of service provision,[148] and for policies, which can address the socioeconomic issues that may be unique to specific regions. It bears noting that in the case of Peru decentralization was based on areas most affected by violence,[149] rather than those judged to have the greatest need for economic assistance. This creates a conceptual discord, as decentralized funding and economic development projects are being employed to remedy widespread violence and violations of civil and political rights, rather than to address the socioeconomic problems for which they were originally designed.[150] Nonetheless, decentralization of the use of collective

143. Roht-Arriaza & Orlovsky, *supra* note 121, at 184.

144. Waldorf, *supra* note 19, at 172.

145. *See, e.g.*, BIX GABRIEL ET AL., TRANSFORMING SITES OF DETENTION: A REVIEW OF AND ROADMAP FOR REPARATIONS AND MEMORIALIZATION IN MOROCCO 9–11 (2013), *available at* http://www.sitesofconscience.org/wp-content/uploads/2013/01/FINAL-MOROCCO-REPORT1.pdf (noting the roles of local and regional governments in the implementation of reparations in Morocco).

146. Roht-Arriaza, *Reparations*, *supra* note 21, at 120.

147. Roht-Arriaza & Orlovsky, *supra* note 121, at 184.

148. *Id.*

149. Roht-Arriaza, *Reparations*, *supra* note 21, at 120.

150. Roht-Arriaza & Orlovsky, *supra* note 121, at 191.

reparations can ensure region-specific spending, which can help to remedy socioeconomic marginalization and strengthen protections of ESRs.

G. Participatory Budgeting and Oversight

Participatory budgeting, closely linked to decentralization, is another potential mechanism for fostering economic and social change, and for fulfilling the ESRs within specific communities. It entails creating a mechanism for community members, through a representative, deliberative process, to decide how public funds designated for a community or region will be spent.[151] It is most effective when combined with a degree of oversight or monitoring by community members into how the projects decided upon are implemented.[152] This Subpart considers examples of participatory budgeting in the transitional justice settings of Guatemala, Peru, and Bolivia.

The likelihood of participatory budgeting succeeding is maximized where the country's national government does not seek to interfere or undermine the process. One example of governmental interference is Guatemala's decentralization reforms, which were outlined in the 1996 Peace Accords before being codified in 2002.[153] The Guatemalan government appeared to adopt these measures mainly because of international pressure or guidance,[154] rather than as part of a good faith effort to give greater power to local decision-making. Consequently, it gave the participatory bodies—municipal councils—mainly administrative obligations, rather than a meaningful opportunity to participate in decision-making.[155] This undermined their potential to alter government spending in ways that would maximize the benefit to communities.

Participatory budgeting policies in Peru and Bolivia have been more successful. Peru's participatory budgeting laws were initiated by President Alejandro Toledo in the context of the democratization of Peru following the rule of President Alberto Fujimori,[156] and were supported by the Peruvian Truth and Reconciliation Commission.[157] The process was lauded for engaging civil society in the debate over the expenditure of public resources, as well as increasing the focus on poverty alleviation projects.[158] Community participation, through election of management

---

151. M.A. Hordijk, *Peru's Participatory Budgeting: Configurations of Power, Opportunities for Change*, 2 OPEN URBAN STUD. J. 43, 43 (2009).

152. *See, e.g., id.* at 53 (comparing the oversight processes of Peru and Brazil's participatory budgeting programs and concluding that even when the oversight process is perceived as weak it nonetheless "enables civil society in general to monitor government's progress" and "offers important opportunities to increase citizens' participation in local decision making").

153. Benjamin Goldfrank, Presentation to the Latin American Studies Association Meeting: Lessons from Latin American Experience in Participatory Budgeting 7 (Mar. 2006), http://www.internationalbudget.org/themes/PB/LatinAmerica.pdf.

154. *Id.* at 26–27.

155. *Id.* at 27.

156. Stephanie McNulty, *An Unlikely Success: Peru's Top-Down Participatory Budgeting Experience*, J. PUB. DELIBERATION, Dec. 30, 2012, art. 4, at 2.

157. Laplante, *supra* note 97, at 354.

158. *See, e.g.*, McNulty, *supra* note 156, at 1 (characterizing Peru's engagement of civil society organizations in the debate as to how to allocate public resources, as well as the increased focus on

committees, led to quick implementation of community-defined projects, most of which targeted socioeconomic needs of communities.[159] At a local level, the Bolivian town of Curahuara de Carangas also benefitted from participatory budgeting, which has reinvigorated indigenous institutions, respect for women,[160] civic associations, and a focus on long-term development and public works and programs.[161]

Despite these successes, some commentators lament that Peru's use of collective reparations as a means of addressing ESRs has occurred at the expense of according reparations processes with a significant degree of meaning and symbolism.[162] Apart from victim confusion about whether such projects were reparative or merely development projects, some members of national government also characterized reparations as tools for addressing the harms caused by terrorism, rather than also addressing the state's culpability for past violations.[163] This illustrates the need for clear and consistent messaging from governments regarding the purpose of participatory budgeting and collective reparations. While exhibiting some pathologies, participatory budgeting programs have the potential to empower and dignify victims, to redress breaches of human rights, and to fulfill ESRs at a local or regional level, especially in situations where specific geographical areas have previously been marginalized.

H. Vetting

A final tool that can be employed in the transitional justice context to remedy breaches of state duties to respect and protect ESRs, and to avoid recurrence of breaches, is the strategic use of vetting procedures. Vetting is usually understood as the process of ensuring that public officials personally responsible for gross violations of human rights do not continue to serve in state employment.[164] For instance, in Bosnia and Herzegovina, close to 24,000 law enforcement officials were screened for involvement in mass atrocities.[165] However, where breaches of ESRs were rife, or were linked to the past conflict, vetting those guilty of ESR violations, including non-state actors, can be an effective means of ensuring non-recurrence and of

---

poverty-reduction projects, as a "success"); *cf.* Goldfrank, *supra* note 153, at 33 (describing in 2006 "a weak, fragmented civil society with little interest in institutionalized participation and little information about the recent laws").

159. CORREA, *supra* note 134, at 12–13.

160. *Cf. id.* at 13 (noting that "the participation of women [in participatory budgeting and implementation] has been notably low" in Peru).

161. Goldfrank, *supra* note 153, at 35.

162. *Cf.* CORREA, *supra* note 134, at 14 (noting a study in which "58 percent of those surveyed did not identify community reparations projects implemented in their communities as reparations").

163. *Id.* at 14.

164. Independent Expert, *Promotion and Protection of Human Rights: Report of the Independent Expert to Update the Set of Principles to Combat Impunity*, principle 36(a), U.N. Doc. E/CN.4/2005/102/Add.1 (Feb. 8, 2005) (by Diane Orentlicher); *see generally* Alexander Mayer-Rieckh, *Vetting to Prevent Future Abuses: Reforming the Police, Courts, and Prosecutor's Offices in Bosnia and Herzegovina*, *in* JUSTICE AS PREVENTION: VETTING PUBLIC EMPLOYEES IN TRANSITIONAL SOCIETIES 180 (Alexander Mayer-Rieckh & Pablo de Greiff eds., 2007).

165. Mayer-Rieckh, *supra* note 164, at 188–91.

strengthening the rule of law. This tactic was employed in Liberia in 2003, following the conclusion of its second Civil War.[166]

The Liberian Truth and Reconciliation Commission found that "root causes" of the civil war included poverty, endemic corruption, and historical disputes over land distribution, all of which undermined access to education, justice, and socioeconomic opportunities.[167] Research has revealed that Liberia's infamous President during the conflict, Charles Taylor, granted timber concessions to increase political strongholds and patronage, to line his own pockets,[168] and even in exchange for arms.[169] The president of one such company, Oriental Timber Corporation, has faced prosecutions by Dutch authorities, which are ongoing, for his involvement in illegal arms deals and for war crimes.[170]

The complicit logging companies operating in Liberia during its five-year civil war, in addition to fueling conflict, also contributed to the violation of the ESRs of individuals and communities. These violations constitute instances of governmental failures to protect ESRs. Individuals were forcibly removed from their land,[171] violating their rights to an adequate standard of living, including rights to suitable housing and food, among others. The companies, emboldened by the lack of government supervision over their activities, also committed widespread violations of national logging regulations, such as clearcutting and the cutting of undersized trees.[172] This led to serious environmental effects, such as land erosion and the destruction of natural fauna habitats, potentially imperiling the land-based livelihoods of local communities.[173] In addition, the logging companies' egregious instances of tax evasion—companies paid only 2 to 3% of all tax due—was described by the Liberian Truth and Reconciliation Commission as widespread and systematic.[174] This affected the government's available resources for development projects, albeit in circumstances where such money may not have been so used.[175] Finally, the logging companies breached contractual obligations to local communities

166. REPUBLIC OF LIBER. TRUTH & RECONCILIATION COMM'N, *supra* note 89, at 18.

167. *Id.* at 16–17.

168. JOHN WOODS ET AL., INVESTMENT IN THE LIBERIAN FOREST SECTOR: A ROADMAP TO LEGAL FOREST OPERATIONS IN LIBERIA 1 (2008), *available at* http://www.forest-trends.org/documents/index.php?pubID=519 ("[Oriental Timber Corporation] paid millions into Charles Taylor's personal bank account; all for which they received tax credit.").

169. Stephanie L. Altman et al., *Leveraging High-Value Natural Resources to Restore the Rule of Law: The Role of the Liberia Forest Initiative in Liberia's Transition to Stability*, *in* HIGH-VALUE NATURAL RESOURCES & POST-CONFLICT PEACEBUILDING 337, 340 (Päivi Lujala & Siri Aas Rustad eds., 2012).

170. Press Release, Global Witness, Global Witness Welcomes Dutch Court Decision to Retry Timber Baron Guus Kouwenhoven for Crimes Committed during Liberian War (Apr. 21, 2010), http://www.globalwitness.org/library/global-witness-welcomes-dutch-court-decision-retry-timber-baron-guus-kouwenhoven-crimes.

171. REPUBLIC OF LIBER. TRUTH & RECONCILIATION COMM'N, *supra* note 89, at 289–90.

172. *Id.* at 290.

173. *See id.* ("[F]orests that are clear cut will not naturally regenerate, rendering the area useless for future forestry.").

174. *Id.*

175. Indeed, liability may not have accrued for breaches of ESRs where circumstances (such as a civil war) exist that render it materially impossible for a state to comply with its international obligations. INT'L LAW COMM'N, DRAFT ARTICLES ON RESPONSIBILITY OF STATES FOR INTERNATIONALLY WRONGFUL ACTS art. 23 (2001), *reprinted in* G.A. Res. 56/83, annex, U.N. Doc. A/Res/56/83 (Jan. 28, 2002).

in the logging areas, which obliged the companies to build hospitals, schools, and infrastructure, and to hire local individuals as unskilled laborers, further impacting local individuals' rights to health, education, and work.[176] While the fulfillment of those rights remains the responsibility of the State, this discussion illustrates the impacts that non-state actors can have on ESRs.

The Liberia Forest Initiative (LFI), a partnership between the government, international organizations, and civil society organizations, was set up in 2004 to collect statements regarding abuses by logging companies and their security forces during the civil war.[177] It then developed vetting processes[178] as part of broader reforms of the timber industry to encourage transparency and equitable and sustainable use of Liberia's forests.[179] A review of all timber concessions was undertaken by a committee staffed by government officials, local civil society organizations, United Nations staff, and LFI partners; this produced findings that all of the seventy existing concessions had been granted illegally.[180] Twelve companies who had previously held concessions were found to have directly participated in the nation's conflict, traded arms for timber, or otherwise aided and abetted social instability.[181] The LFI profited from a newly installed government that was willing to institute the necessary reforms to set up a robust system aimed at preventing future recurrence of conflict, which had previously been fueled and financed by "conflict timber" as well as "blood diamonds."[182] The government declared all of the existing timber concessions null and void, and it embarked on creating a new process for granting concessions.[183] According to the new process, a company that has been suspended or debarred, for example because of criminal convictions or failures to pay tax, is ineligible to bid for future tenders,[184] and individuals with significant interests in companies involved in logging in Liberia prior to 2006 are required to file sworn statements setting out their involvement, and to cooperate with the government in recouping lost funds caused by illegal activity.[185]

176. REPUBLIC OF LIBER. TRUTH & RECONCILIATION COMM'N, *supra* note 89, at 290 ("[T]he University of Liberia granted 284,000 acres of University forest to [Oriental Trading Company], in exchange for $2 million USD in renovations to the University of Liberia and 50% of profits, according to President Taylor. No payments were ever made.").

177. *About the Liberia Forest Initiative*, FOOD & AGRIC. ORG., http://www.fao.org/forestry/lfi/29021/en/ (last visited June 15, 2015).

178. Duthie, *supra* note 3, at 189.

179. Altman et al., *supra* note 169, at 337.

180. *See id.* at 344–45 (noting that no Liberian timber concession granted met all four criteria necessary to maintain the concession).

181. *Id.* at 345. While not constituting ESR violations per se, the companies' actions had severe economic and social consequences, as discussed below.

182. Altman et al., *supra* note 169, at 340.

183. *Id.* at 337.

184. *See, e.g.*, WOODS ET AL., *supra* note 168, at 4 ("Firstly, companies must not be suspended or debarred from bidding, for example, because of tax arrears or criminal convictions. Secondly, the company must demonstrate that it is incorporated; involved with logging; has a main office in Monrovia; the officers/directors have not been penalized for violating corporate- or forestry-laws, and have not declared bankruptcy; and that the company is in good standing in payment of taxes, social security, forest- and trade-fees.").

185. *Id.*

Commercial vetting can also impact the integrity of a country's legal system, and should thus be contemplated with caution. For instance, opportunistic members of a post-conflict government may seek to vet economic actors and repudiate existing government contracts for improper purposes such as granting favors or encouraging new patronage networks. This could adversely impact a country's economy, as investors perceive a lack of commercial certainty and legal integrity. A country could also face arbitration or litigation. A vetted company may seek to sue a country for breach of an investment contract or for protection from state expropriations of their investments pursuant to international investment or trade treaties[186] that ensure the rights of corporations to wide-reaching standards like "fair and equitable treatment."[187] Litigation for breaches of investment can lead to large compensation orders against States,[188] which can seriously deplete public funds available for socioeconomic services. This underlines the importance of carrying out vetting programs through transparent and principled processes.[189] In this regard, the LFI's engagement with a broad range of types of organizations helped to ensure a robust and principled vetting process. To avoid litigation, such programs should also be designed so as to meet the requirements for legal repudiation of such contracts and with the goal of exposing illegal and corrupt practices, which can better protect the country from being sued by the investor under investment or trade treaties.[190]

While the LFI's vetting policy is linked to the past civil conflict, it is illustrative of the role vetting can play in excluding individuals or corporations against which credible allegations of corruption, tax evasion,[191] or other economic violence exist. Such violations affect a State's ability to respect, protect, and fulfill ESRs by eroding state revenue and denying affected landholders and occupiers due process. When coupled with broader sector reforms, vetting will often have a productive role to play

186. *E.g.*, Central America-United States Free Trade Agreement arts. 10.7, 10.16, Aug. 5, 2004, 43 I.L.M. 513.

187. *See, e.g.*, North American Free Trade Agreement art. 1105, Dec. 17, 1992, 32 I.L.M. 289 (guaranteeing investors "treatment in accordance with international law, including fair and equitable treatment"); Lise Johnson and Oleksandr Volkov, *Investor-State Contracts, Host-State "Commitments" and the Myth of Stability in International Law*, 24 AM. REV. INTL ARB. 361, 379 (2013) ("A number of [investor-state dispute settlement] cases have gone further and determined that when states contract with foreign investors, the *existence* of the regulatory framework gives rise to an *implied* promise that the investment will not be impacted by subsequent regulatory change." (emphasis in original))

188. For instance, Pac Rim Cayman LLC is currently suing the state of El Salvador for $300,000 in compensation after the government refused to grant the company permission to commence a gold mine. Pac Rim Cayman LLC v. Republic of El Sal., ICSID Case No. ARB/09/12 (2009).

189. While a principled process in itself will not immunize a State from the prospect of investor-state dispute settlement, the transparent process in Liberia's case revealed the primary motivation for the country's vetting was the illegal and corrupt practices of corporate actors. *See* REPUBLIC OF LIBER. TRUTH & RECONCILIATION COMM'N, 2 CONSOLIDATED FINAL REPORT 336–37, 372 (2009). This could enliven an emerging defense for host States, based on a company's involvement in corrupt practices. *See, e.g.*, Jason Yackee, *Investment Treaties and Investor Corruption: An Emerging Defense for Host States?*, INVESTMENT TREATY NEWS (Oct. 19, 2012), https://www.iisd.org/itn/2012/10/19/investment-treaties-and-investor-corruption-an-emerging-defense-for-host-states/ (discussing the agreement of Siemans, A.G. not to enforce a $200 million arbitral award against Argentina after the company was found to be heavily implicated in an international practice of bribing public officials).

190. *See* Yackee, *supra* note 189 (noting the "potential benefits of a corruption defense" for host States through the example of *Siemans, A.G.*).

191. The seventy logging companies in Liberia were later found to be "US$64 million in tax arrears." WOODS ET AL., *supra* note 168, at 2.

in preventing the future mismanagement of a nation's environmental resources, and the depletion of its tax reserves. This example also illustrates the overlap of, and thus the need for greater coordination and interfacing between, the fields of transitional justice and business and human rights. The unique opportunity of transitional contexts to redefine legal cultures should be used not only to address state human rights obligations, but also to set out appropriate legal protections and regulatory programs to ensure that business activities do not adversely affect the ESRs of community members. The prospect of extending the obligations of businesses with regard to human rights beyond those set out in the 2011 Guiding Principles,[192] upon which a United Nations Working Group has been tasked to begin consulting,[193] may also create additional challenges and opportunities for the field of transitional justice.

CONCLUSION

It is anachronistic to consider ESRs as outside the bounds of transitional justice. Doing so risks skewing understandings of past atrocities, which in turn affects transitional justice's ability to prevent their recurrence. This Article has sought to contribute to the field of transitional justice by reinforcing the indivisibility of ESRs, and by analyzing some of the broader transitional justice mechanisms that States can employ to meet their ESR obligations during transitional periods. Determining which types of rights should or should not be included in a particular case will depend on the facts on the ground and the capacities of the specific transitional justice mechanism concerned. However, such decisions should not be guided by erroneous notions of ESRs as being less important than civil and political rights. Government failures to respect and protect ESRs are generally discrete enough to be included, where relevant, in the mandates of truth commissions, prosecutions, reparations programs, and vetting processes. Breaches of state obligations to fulfill human rights in specific communities or regions can be addressed in some instances: Truth commissions can acknowledge such failures and recommend appropriate reforms; reparations can remedy the effects of failures to fulfill ESRs on a limited scale; and collective reparations and decentralized governance processes can empower communities to more actively direct the course of their development and respond to socioeconomic issues that may have been ignored by previous national government policies. Similarly, vetting processes can improve the government's ability to fulfill ESRs by excluding public and private actors whose practices eroded public funds, damaged socioeconomic infrastructure and services, or otherwise negatively affected a population's ESRs. Such breaches should therefore not be automatically excluded from truth commission mandates or other transitional justice procedures. Widespread or nationwide failures to fulfill ESRs, on the other hand, may be more difficult for transitional justice mechanisms to address. Nonetheless, transitional contexts present unique opportunities for reinvention of legal and political cultures. To automatically exclude consideration of ESRs—even state

192. Special Representative of the Secretary-General, *Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework: Rep. of the Special Representative of the Secretary-General on the Issue of Human Rights and Transnational Corporations and Other Business Enterprises*, U.N. Doc. A/HRC/17/31 (Mar. 21, 2011) (by John Ruggie).

193. H.R.C. Res. 26/22, para. 7, U.N. Doc. A/HRC/RES/26/22 (July 15, 2014).

obligations to fulfill ESRs—at such a moment in a nation's history is to miss an important opportunity for the improvement of a nation's socioeconomic conditions and the strengthening of its commitment to all human rights. Ultimately, transitional justice can no longer ignore that ESRs articulate non-negotiable and clearly defined standards, which often hold the key to stable and sustainable transitions.

A Judgment Without Merits: The Recognition and Enforcement of Foreign Judgments Confirming, Recognizing, or Enforcing Arbitral Awards

BURTON S. DEWITT*

TABLE OF CONTENTS

* J.D., University of Texas School of Law 2015; B.A. History and Medieval Studies, Rice University 2010. I would like to thank Professor Alan Scott Rau for his help in this Note, as well as Garrett Martin, Becca Bennie, and all my teammates on the Willem C. Vis moot team for introducing me to arbitration. I would also like to thank the staff of the *Texas International Law Journal*, and especially Rebekah Sills, Jordan Hunn, and Taylor Markway for their work on this Note, as well as Jeffrey Zerda for making sure no 7uagmires sneaked in. Any mistakes remaining are my own.

"Any private mechanism of dispute resolution . . . depends in the last resort on public sanctions and the public monopoly of force."[1] But whose public do we mean? Or, to be more precise, the public legal system of which country? Obviously, a judgment by a court confirming, setting aside, recognizing, or enforcing an arbitral award would bind the applicable parties to its judgment within that jurisdiction. And in the United States, full faith and credit would mandate that other American courts give the same credence to the judgment as did the rendering court.[2] But while much has been written on the effect of foreign judgments setting aside arbitral awards at the seat,[3] the effect of a foreign judgment confirming, recognizing, or enforcing an arbitral award has until recently been greatly ignored.[4] This is despite courts in various jurisdictions enforcing these judgments in lieu of the underlying award.[5]

It is well settled in the United States that a foreign judgment confirming an arbitral award can be enforced by American courts.[6] This is especially true when the award and judgment were both rendered in the primary jurisdiction,[7] but the extent of deference is so undefined that at least one court has found a claim to set aside an American-seated award precluded after a Canadian court recognized the award in the interim.[8] Regardless of the wisdom of deferring to the foreign judgment in any situation, it is hard to say U.S. courts have completely missed the boat. Both the 2005 Uniform Foreign-Country Money Judgments Recognition Act[9] and the proposed Foreign Judgments Recognition and Enforcement Act[10] explicitly apply to some foreign judgments on arbitral awards, indicating at the very least an inclination among many academics and the bar to view such judgments as ordinary judgments.

---

1. Alan Scott Rau, *Understanding (and Misunderstanding) "Primary Jurisdiction,"* 21 AM. REV. INT'L ARB. 47, 48 (2010).

2. U.S. CONST. art. IV, § 1; *accord* Estin v. Estin, 334 U.S. 541, 544–46 (1948).

3. *E.g.*, Albert Jan van den Berg, *Enforcement of Arbitral Awards Annulled in Russia: Case Comment on Court of Appeal of Amsterdam, April 28, 2009*, 27 J. INT'L ARB. 179 (2010); Kenneth R. Davis, *Unconventional Wisdom: A New Look at Articles V and VII of the Convention on the Recognition and Enforcement of Foreign Arbitral Awards*, 37 TEX. INT'L L.J. 43 (2002); Günther J. Horvath, *What Weight Should Be Given to the Annulment of an Award under the* Lex Arbitri*? The Austrian and German Perspectives*, 26 J. INT'L ARB. 249 (2009); Philippe Pinsolle, *The Status of Vacated Awards in France: The Cour de Cassation Decision in* Putrabali, 24 ARB. INT'L 277 (2008).

4. *Cf.* Maxi Scherer, *Effects of Foreign Judgments Relating to International Arbitral Awards: Is the 'Judgment Route' the Wrong Road?*, 4 J. INT'L DISP. SETTLEMENT 587, 588 & n.5 (2013) (acknowledging that the issue "has attracted little attention in scholarly writing").

5. *See infra* Part III.

6. It is also well settled that the New York Convention on the Recognition and Enforcement of Foreign Arbitral Awards ("New York Convention" or "Convention") obviated the need for a court in the primary jurisdiction to confirm the award as a condition precedent to recognition and enforcement in a secondary jurisdiction. *See, e.g.*, Yusuf Ahmed Alghanim & Sons v. Toys "R" Us, Inc., 126 F.3d 15, 22 (2d Cir. 1997) ("The Convention eliminated this problem by eradicating the requirement that a court in the rendering state recognize an award before it could be taken and enforced abroad.").

7. *See, e.g.*, Seetransport Wiking Trader Schiffahrtsgesellschaft MBH & Co., Kommanditgesellschaft v. Navimpex Centrala Navala, 29 F.3d 79, 82 (2d Cir. 1994) (holding that a French decree conferring *exequatur* on a French arbitral award amounted to an enforceable judgment under New York law, but expressing doubt that the "award-without-*exequatur*" would be an enforceable judgment).

8. Belmont Partners, LLC v. Mina Mar Grp., 741 F. Supp. 2d 743, 753 (W.D. Va. 2010).

9. UNIF. FOREIGN-COUNTRY MONEY JUDGMENTS RECOGNITION ACT § 2 cmt. 3 (2005).

10. FOREIGN JUDGMENTS RECOGNITION & ENFORCEMENT ACT § 1(a)(iii) (Proposed Act 2005).

In this Note, I will address the deference U.S. courts should give to foreign judgments confirming, recognizing, or enforcing arbitral awards.[11] In Part I, I will look at the legal framework under which U.S. courts operate to enforce foreign awards and judgments. In Part II, I will turn to foreign judgments confirming, recognizing, or enforcing arbitral awards. I will argue that they are cognizable under U.S. law relating to foreign judgments, regardless of their enforceability. Finally, in Part III, I will address the enforceability and preclusive value in the United States of foreign judgments confirming, recognizing, or enforcing arbitral awards. I will first argue that due to their ancillary nature, they are not enforceable. However, I will also argue that under certain circumstances, foreign judgments can be preclusive of certain issues actually litigated in the foreign forum.

I. THE ENFORCEABILITY OF FOREIGN AWARDS AND JUDGMENTS IN THE UNITED STATES

Suits to confirm or set aside arbitral awards are guided by different legal principles than suits to recognize and enforce foreign judgments and give them preclusive effect. In the following Subparts, I will briefly introduce the prerequisites for and limitations on both issues.

A. The Enforceability of Foreign Awards

Since 1970, the United Nations Convention on the Recognition and Enforcement of Foreign Arbitral Awards ("New York Convention" or "Convention")[12] has been the primary guiding force with respect to foreign arbitral award enforcement in the United States.[13] Except as limited by a Contracting State,[14] a foreign arbitral award must be recognized and enforced under the New York Convention unless it meets one of the enumerated grounds to deny recognition and

11. There are four different types of proceedings that may be brought by a party concerning an arbitral award: set aside, confirmation, recognition, and enforcement. *E.g.*, Linda J. Silberman & Maxi Scherer, *Forum Shopping and Post-Award Judgments* 313, 313 (N.Y. Univ. Sch. of Law Pub. Law & Legal Theory Research Paper Series, Working Paper No. 13-77, 2013). Confirmation occurs when an award is deemed valid and effective at the seat (or, alternatively, a judgment at the seat "refusing to set aside an award"). *Id.* at 336. Recognition occurs when any court acknowledges the validity of an award. *Id.* at 330. Enforcement occurs when either a court at the seat or a court in a foreign state—after either confirming or recognizing the award—renders a judgment that makes the award collectable from the debtor's property within that state. *Id.* The enforcement of foreign judgments setting aside arbitral awards is beyond the scope of this Note.

12. United Nations Convention on the Recognition and Enforcement of Foreign Arbitral Awards, *opened for signature* June 10, 1958, 21 U.S.T. 2517, 330 U.N.T.S. 38 [hereinafter New York Convention].

13. *See, e.g.*, Victrix S.S. Co. v. Salen Dry Cargo A.B., 825 F.2d 709, 712–13 (2d Cir. 1987) ("[T]he [New York] Convention preempts state laws and leaves the entire subject of enforcement of foreign arbitration awards governed by its terms."). *But see* Weizmann Inst. of Sci. v. Neschis, 421 F. Supp. 2d 654, 674 (S.D.N.Y. 2005) ("The Convention does not appear to preempt all other law governing the recognition of foreign arbitral awards or to bar the recognition of awards not falling under the Convention, including awards from non-signatory states such as Liechtenstein.").

14. *See* New York Convention, *supra* note 12, art. I.3 (allowing a Contracting State to limit the scope of the Convention to only recognize commercial awards or awards from other Contracting States if a State so chooses).

enforcement.[15] Upon motion of the party against whom enforcement is sought, a U.S. court can refuse recognition if: (a) the party shows that arbitration was not validly agreed to under the applicable law; (b) the party shows that it lacked notice or was not provided an opportunity to present its case; (c) the award exceeded the scope of the agreement to arbitrate; (d) the composition of the arbitral tribunal either was not in accord with the parties' agreement or the law of the place of arbitration; or (e) the award is not binding or has been set aside by or under the law of the seat.[16] Additionally, a U.S. court may refuse to recognize and enforce the award if the court determines that U.S. law deems the dispute unable to be settled by arbitration, or if recognition and enforcement would be contrary to U.S. public policy.[17] In the somewhat rare situation where an award is not subject to the New York Convention—for instance, the award was rendered in a non-contracting country—a U.S. court may enforce it under the Federal Arbitration Act.[18]

Two of the discretionary grounds to refuse enforcement of a foreign arbitral award are intricately tied to the law of the foreign state in which the award was rendered. First, a court may refuse enforcement where the arbitration agreement violated the applicable law.[19] Second, a foreign court may refuse to enforce an arbitral award that is either not final or has been set aside at the seat.[20] However, these grounds do not *require* non-recognition: A court may still choose to recognize a foreign arbitral award even if it finds a ground for refusing recognition.[21] Nothing in the New York Convention mandates that a foreign court refuse to enforce an arbitral award, although a court must enforce the award in the absence of a ground to refuse enforcement.[22]

These grounds to refuse to recognize and enforce foreign arbitral awards should not be confused with the primary jurisdiction's right to set aside arbitral awards outside of the Convention. By its very terms, the New York Convention only applies "to the recognition and enforcement of arbitral awards made in the territory of a State other than the State where the recognition and enforcement of such awards are sought."[23] Thus, a suit to confirm or set aside an award would be subject to an

---

15. *Id.* art. V.

16. *Id.* art. V.1.

17. *Id.* art. V.2.

18. *Cf.* Cortez Byrd Chips, Inc. v. Bill Harbert Constr. Co., 529 U.S. 193, 202–03 (2000) (addressing how an improperly narrow reading of the Federal Arbitration Act would preclude its use to confirm, modify, or vacate awards not subject to the Convention).

19. New York Convention, *supra* note 12, art. V.1(a). A recent example may be France's treatment of unilateral jurisdiction clauses, where one party can resort to courts in lieu of arbitration, while the other party is limited to commencing arbitration. *See generally* Deyan Draguiev, *Unilateral Jurisdiction Clauses: The Case for Invalidity, Severability or Enforceability*, 31 J. INT'L ARB. 19 (2014).

20. New York Convention, *supra* note 12, art. V.1(e). An award may not be final if there is a pending appeal of some sort (or the time to appeal the award has not elapsed). Whether an award is final and binding should be determined "by the law of the State in which, or under the law of which, the award was made." U.N. Comm'n on Int'l Trade Law, Rep. on the Work of Its Eighteenth Session, June 3–21, para. 313, U.N. Doc. A/40/17; GAOR, 40th Sess., Supp. No. 17 (1985).

21. France is the most notorious for this, enforcing arbitral awards despite their being set aside at the seat. *Infra* note 143 and accompanying text.

22. New York Convention, *supra* note 12, art. III.

23. *Id.* art. I.1.

entirely different set of obligations than a suit to recognize and enforce an arbitral award rendered in a foreign country.

B. The Enforceability of Foreign Judgments

Unlike the recognition and enforcement of foreign arbitral awards, foreign judgments are recognized and enforced according to state law or federal common law.[24] Attempts to unify state law have been moderately successful, and the majority of states now follow either the 1962 Uniform Foreign Money-Judgments Recognition Act ("1962 Uniform Act") or the 2005 Uniform Foreign-Country Money Judgments Recognition Act ("2005 Uniform Act").[25] One or both of these Uniform Acts have been enacted in almost every major hub of international business, including California,[26] Illinois,[27] New York,[28] Texas,[29] and Washington, D.C.[30] Nonetheless, attempts to unify and codify a federal standard have floundered. A proposed act by the American Law Institute in 2006 nearly fell apart,[31] while academics have forwarded various different proposals for a uniform federal law.[32] Thus, despite similarities throughout the United States on the enforceability of foreign judgments, minor differences can be found.[33]

The 1962 Uniform Act left ambiguous whether and to what extent it applied to judgments confirming and vacating arbitral awards. It specifically applied to any foreign judgment that was "final and conclusive and enforceable,"[34] defining foreign judgment as "any judgment of a foreign state granting or denying recovery of a sum of money," excluding judgments for taxes, fines, and family law matters.[35] Any such foreign judgment was entitled to the same deference as a judgment of a different

---

24. *See, e.g.*, McCord v. Jet Spray Int'l Corp., 874 F. Supp. 436, 439–40 (D. Mass. 1994) (applying Massachusetts's reciprocity requirement for recognition of foreign judgments in a diversity jurisdiction case).

25. Thirty-one states adopted the 1962 version. *Legislative Fact Sheet - Foreign Money Judgments Recognition Act*, UNIFORM L. COMM'N, http://www.uniformlaws.org/LegislativeFactSheet.aspx?title=Foreign%20Money%20Judgments%20Recognition%20Act (last visited Apr. 3, 2015). Nineteen states—including seventeen that had previously adopted the 1962 version—have adopted the 2005 version. *Legislative Fact Sheet - Foreign-Country Money Judgments Recognition Act*, UNIFORM L. COMM'N, http://www.uniformlaws.org/ LegislativeFactSheet.aspx?title=Foreign-Country%20Money%20Judgments%20Recognition%20Act (last visited Apr. 3, 2015).

26. CAL. CIV. PROC. CODE §§ 1713–1724 (West Supp. 2015).

27. 735 ILL. COMP. STAT. 5/12-650 to -657 (West 2011 & Supp. 2014).

28. N.Y. C.P.L.R. §§ 5301–5309 (McKinney 2014).

29. TEX. CIV. PRAC. & REM. CODE ANN. §§ 35.001–.007 (West 2015).

30. D.C. CODE §§ 15-361 to -371 (2013).

31. *See* Stephen B. Burbank, *A Tea Party at the Hague?*, 18 SW. J. INT'L L. 629, 640 & n.56 (2012) (suggesting that the 2006 Uniform Law was designed, at least in part, to sabotage the Model Law project).

32. *See generally* Yuliya Zeynalova, *The Law on Recognition and Enforcement of Foreign Judgments: Is It Broken and How Do We Fix It?*, 31 BERKELEY J. INT'L L. 150 (2013) (proposing a uniform federal law based on the failed 2006 law, which would preempt state law).

33. *Cf.* Ronald A. Brand, *Federal Judicial Center International Litigation Guide: Recognition and Enforcement of Foreign Judgments*, 74 U. PITT. L. REV. 491, 500–04 (2013) (comparing the various state laws on foreign judgment recognition and enforcement).

34. UNIF. FOREIGN MONEY-JUDGMENTS RECOGNITION ACT § 2 (1962).

35. *Id.* § 1(2).

U.S. state unless one of nine exceptions applied.[36] The 1962 Uniform Act is remarkably short, totaling just eleven sections over five pages and only four notes,[37] and thus offers little explanatory guidance. However, its influence is unquestionable, as it was adopted by thirty-one states as well as the District of Columbia and the U.S. Virgin Islands.[38]

The 2005 Uniform Act resolves the ambiguity over foreign judgments confirming or vacating arbitral awards, expressly stating that such judgments are covered by the Act.[39] It does not discuss judgments recognizing and enforcing arbitral awards.[40] Beyond changing the term from foreign judgment to foreign-country judgment, the Act defines foreign-country judgment broadly as "a judgment of a court of a foreign country,"[41] although a subsequent section provides the same limitations on the scope of the Act as the 1962 version.[42] It contains most of the same grounds for non-recognition and non-enforcement as the 1962 Act.[43] The 2005 Uniform Act has been enacted in nineteen states and the District of Columbia, and is currently introduced in several other state legislatures.[44]

Furthermore, these acts appear to be consistent with the Restatement (Third) of Foreign Relations Law. The Restatement may be guiding even in states that have adopted one of the Uniform Acts, as any foreign judgment that does not meet the Uniform Act's definition of a foreign judgment or scope of applicability can still be recognized and enforced through common law principles.[45] The Restatement

---

36. *Id.* §§ 3–4. The 1962 Act provides that a judgment is not conclusive and therefore not enforceable if the judgment came from a tribunal lacking procedures compatible with due process of law, was rendered without personal jurisdiction over the judgment debtor, or was rendered without jurisdiction over the subject matter of the dispute. *Id.* § 4(a). Moreover, a U.S. court has discretion in enforcing a foreign judgment in six cases: (a) the judgment debtor lacked notice in the foreign proceedings; (b) the judgment was obtained by fraud; (c) either the judgment's cause of action or the claim for relief is repugnant to the public policy of the state where enforcement is sought; (d) the judgment conflicts with another otherwise enforceable judgment; (e) the foreign judgment was rendered contrary to an agreement between the parties to settle the dispute by a different means; or (f) jurisdiction was valid only because of personal service, but the forum was nonetheless a "seriously inconvenient" one. *Id.* § 4(b).

37. *See generally id.*

38. *Legislative Fact Sheet - Foreign Money Judgments Recognition Act*, UNIFORM L. COMM'N, http://www.uniformlaws.org/LegislativeFactSheet.aspx?title=Foreign%20Money%20Judgments%20Recognition%20Act (last visited Apr. 3, 2015).

39. UNIF. FOREIGN-COUNTRY MONEY JUDGMENTS RECOGNITION ACT § 2 cmt. 3 (2005).

40. *Id.*

41. *Id.* § 2(2).

42. *Id.* § 3. This section is meant to mimic the definition of "foreign judgment" under the 1962 Act. *See id.* § 3 cmt. Source ("This section is based on Section 2 of the 1962 Act. Subsection (b) contains material that was included as part of the definition of 'foreign judgment' in Section 1(2) of the 1962 Act.").

43. The 2005 Uniform Act contains the same nine grounds for refusing enforcement of the foreign judgment as the 1962 Act, as well as giving a U.S. court discretion to refuse to enforce a judgment "rendered in circumstances that raise substantial doubt about the integrity of the rendering court with respect to the [specific] judgment" or where the "specific proceeding in the foreign court leading to the judgment was not compatible with the requirements of due process of law." *Id.* § 4.

44. *Legislative Fact Sheet - Foreign-Country Money Judgments Recognition Act*, UNIFORM L. COMM'N, http://www.uniformlaws.org/LegislativeFactSheet.aspx?title=Foreign-Country%20Money%20Judgments%20Recognition%20Act (last visited Apr. 3, 2015).

45. *See, e.g.*, Brown's Inc. v. Modern Welding Co., 54 S.W.3d 450, 453 (Tex. App. 2001) ("Texas recognizes two methods of enforcing a foreign judgment: (1) filing under the [1962 Uniform Act] . . . and (2) filing a common-law action to enforce the foreign judgment." (citation omitted)).

explains that a final judgment granting or denying recovery of a sum of moneys is recognizable and enforceable within any court in the United States.[46] It lists exceptions that are similar to the statutory acts.[47] Neither the Restatement nor the reporter notes discuss the recognizability or enforceability of judgments confirming arbitral awards.[48]

Although these acts and the common law may provide for the recognition and enforcement of foreign judgments confirming, recognizing, or enforcing arbitral awards, they do not provide guidance as to what preclusive value these judgments should have or what exactly it is that is being recognized or enforced. We thus turn to those issues now.

II. RECOGNITION OF FOREIGN JUDGMENTS

Recognition of a foreign judgment is not the same thing as enforcement. Recognition is a necessary precondition to enforcement, but it is hardly sufficient.[49] Frequently, and quite possibly in the vast majority of situations, a party seeking recognition will also seek enforcement in the same proceedings.[50] But recognition in the absence of enforcement is significant because cognizance of the award enables the court to preclude relitigation of the cause of action or of particular issues that were litigated in the foreign judgment.[51] Recognition is thus usually part of a party's defense, while enforcement is an action in and of itself.[52] However, the extent to

46. RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW § 481 (1987).

47. Like the Uniform Acts, the Restatement prevents recognizing a judgment rendered in a system without impartial tribunals or lacking in due process, as well as if the foreign court lacked jurisdiction over the judgment debtor. *Id.* § 482(1). Furthermore, the court could refuse recognition in any of six situations: (a) the foreign court lacked subject matter jurisdiction; (b) the defendant did not receive sufficient notice of the foreign proceedings; (c) the judgment was obtained by fraud; (d) the cause of action or the judgment itself is repugnant to the public policy of either the United States or the particular state where enforcement is sought; (e) the judgment conflicts with a different final judgment that otherwise is entitled to recognition; or (f) the proceeding was contrary to an agreement between the parties to resolve their dispute in a different forum. *Id.* § 482(2).

48. *See id.* §§ 481, 482, 487 (failing to discuss foreign judgments confirming arbitral awards).

49. *See, e.g.*, *id.* § 481 cmt. b. ("The judgment of a foreign state may not be enforced unless it is entitled to recognition."); *cf.* RESTATEMENT (SECOND) OF CONFLICT OF LAWS § 98 (1971) ("A valid judgment rendered in a foreign nation after a fair trial in a contested proceeding will be recognized in the United States so far as the immediate parties and the underlying cause of action are concerned."). *But see* Soc'y of Lloyd's v. Ashenden, 233 F.3d 473, 481 (7th Cir. 2000) (interpreting Illinois law to not require a "separate step of 'recognition'" before enforcement).

50. *E.g.*, Royal Bank of Can. v. Trentham Corp., 665 F.2d 515, 515 (5th Cir. Unit A Dec. 1981).

51. *See, e.g.*, Pan. Processes, S.A. v. Cities Serv. Co., 796 P.2d 276, 291–92 (Okla. 1990) (applying res judicata to a defense available under Brazilian law that was not raised in the Brazilian judgment after recognizing the judgment). *Panama Processes* provides a great analysis of the various grounds for refusing to recognize a foreign judgment. The Oklahoma Supreme Court could not apply the 1962 Uniform Act because the Brazilian judgment did not grant or deny recovery of a sum of money. *Id.* at 282 n.21. Nonetheless, the court found the judgment cognizable as a matter of policy after engaging in almost five pages of analysis. *Id.* at 282–87. The opinion is also instructive in choice of law issues.

52. *See, e.g.*, Robert L. McFarland, *Federalism, Finality, and Foreign Judgments: Examining the ALI Judgments Project's Proposed Federal Foreign Judgments Statute*, 45 NEW ENG. L. REV. 63, 71–72 (2010) ("Unlike the offensive context of enforcement, whereby a judgment creditor solicits the state's coercive powers to secure collection, the context of recognition is usually defensive, whereby a litigant seeks to preclude relitigation of claims or issues previously decided elsewhere."). At its simplest, the distinction is

which a foreign judgment precludes further litigation must be determined by the U.S. court.[53] Thus, to fully understand recognition of foreign judgments, we must also take a look at preclusion.

Preclusion under U.S. law can take various shapes depending on the overlap of issues between the two proceedings and upon the extent to which the rendering court relied on the particular issue in its disposition of the matter. Preclusion is generally a matter of state law,[54] although federal courts have developed their own common law of preclusion for federal question cases.[55] At one end of the spectrum is res judicata, or claim preclusion,[56] which prevents parties from relitigating the same dispute that has already been litigated between them.[57] This would include both the matters actually litigated as well as any possible claims or issues that the parties chose not to

---

extremely important. Let us assume Randall sued Smith in Canada and won ten dollars. Smith paid Randall immediately. Randall then brings suit in Travis County, Texas alleging the same incident and same facts that led to the foreign judgment in Canada. Certainly the Travis County court would have to recognize the judgment. The judgment would be res judicata to a subsequent suit for damages and it would be issue preclusive as to any fact determined within the Canadian judgment that was necessary to the judgment. However, when it comes to enforcing the award, Smith would have an affirmative defense because he already paid the ten dollars. There would be, in short, nothing that the court is capable of enforcing.

53. *See, e.g.*, Evans Cabinet Corp. v. Kitchen Int'l, Inc., 593 F.3d 135, 142 n.8 (1st Cir. 2010) ("[I]n the case of recognition to preclude further litigation, once the foreign judgment is deemed entitled to recognition under the Recognition Act, the extent of the foreign judgment's preclusive effect still must be determined.").

54. *See, e.g.*, Semtek Int'l Inc. v. Lockheed Martin Corp., 531 U.S. 497, 507–08 (2001) (holding that because there is no statutory federal preclusion law, the federal law incorporates state preclusion law as federal law in diversity actions); *see also* Dupasseur v. Rochereau, 88 U.S. (21 Wall.) 130, 135–36 (1875) (discussing Louisiana preclusion law in the context of deference to a federal judgment); Stephen B. Burbank, Semtek, *Forum Shopping, and Federal Common Law*, 77 NOTRE DAME L. REV. 1027, 1047–48 (2002) (discussing *Semtek*'s mandate to determine what preclusive effect California law would give a judgment). But for a seminal article arguing in favor of a federal standard for preclusion, at least in regards to preclusion of federal judgments, see Ronan E. Degnan, *Federalized Res Judicata*, 85 YALE L.J. 741 (1976).

55. *See, e.g.*, Allen v. McCurry, 449 U.S. 90, 94–96 (1980) (discussing how federal courts have treated various types of preclusion issues). More accurately, the federal judiciary has created a federal common law of preclusion for all federal judgments, although where state law provides the rule of decision this generally requires the incorporation of state preclusion law as the federal law. *Semtek*, 531 U.S. at 508–09; *cf.* Burton S. DeWitt, Note, *The Application and Construction of the Federal Rules of Evidence in Cases Where State Law Provides the Rule of Decision*, 34 REV. LITIG. (forthcoming Spring 2015) (manuscript at 26 n.150, on file with author) (discussing the analytical difference between reading a federal rule of evidence as incorporating state law from the alternative of deferring to state law). For a discussion of the preclusive effect of a federal judgment where state law provides the rule of decision, see Patrick Woolley, *The Sources of Federal Preclusion Law after* Semtek, 72 U. CIN. L. REV. 527 (2003).

56. Some have equated res judicata to claim preclusion, although others have attempted to distinguish claim preclusion as a subset of res judicata. *See, e.g.*, Taylor v. Sturgell, 553 U.S. 880, 892 (2008) ("The preclusive effect of a judgment is defined by claim preclusion and issue preclusion, which are collectively referred to as 'res judicata.'"); Mason v. State, 206 S.W.3d 869, 874–75 (Ark. 2005) (recognizing that res judicata has been equated to claim preclusion, but distinguishing claim preclusion as a facet of res judicata); Victoria L. Hooper, *Avoiding the Trap of* Res Judicata*: A Practitioner's Guide to Litigating Multiple Employment Discrimination Claims in the Third Circuit*, 45 VILL. L. REV. 743, 743 n.2 (2000) (listing sources that have equated the terms). Whether they are the same is irrelevant for our purposes, as in all situations where there is res judicata, there would also be claim preclusion of at least some issues.

57. *Allen*, 449 U.S. at 94.

raise in the original proceedings, if the rendering jurisdiction would treat those issues as forfeited.[58] Claim preclusion bars a party from bringing the same cause of action that he previously brought if he had received a final adjudication on the merits.[59] While there is no satisfactory and complete definition of cause of action, it generally requires some "essential similarity [in] the underlying events giving rise to the various legal claims," even if the claims arise from different statutory or common law grounds.[60] However, res judicata generally can only bar a claim where the tribunal that issued the would-be preclusive judgment would also find that previous judgment preclusive.[61]

Collateral estoppel, or issue preclusion, has been described as the narrower first cousin of res judicata.[62] It does not bar an entire claim; rather, its scope is limited to a particular issue that the parties have fully litigated in a prior, different cause of action between the parties.[63] Where such an issue has been so litigated, that issue will be treated as established fact in the subsequent proceedings, relieving the proponent from having to relitigate and re-prove its existence, but only if the fact was necessary or essential to the determination of the original cause of action.[64] This last factor—necessity or essentiality—requires the court to ascertain which facts in the first judgment were required to reach that judgment.[65]

---

58. *E.g.*, LA. REV. STAT. ANN. § 13:4231 (West 2014); Benedict v. Snead, 560 S.E.2d 278, 279 (Ga. Ct. App. 2002) ("[W]here there is identity of parties and subject matter, res judicata bars relitigation of matters that were or could have been litigated in an earlier action."). This is in line with most common law systems. *See* Jonathan Hill, *The Significance of Foreign Judgments Relating to an Arbitral Award in the Context of an Application to Enforce the Award in England*, 8 J. PRIVATE INT'L L. 159, 162 n.4 (2012) ("Most common law systems have a doctrine of *res judicata* which comprises both cause of action and issue estoppel.").

59. *E.g.*, *Mason*, 206 S.W.3d at 875; *cf.* Stavros Brekoulakis, *The Effect of an Arbitral Award and Third Parties in International Arbitration: Res Judicata Revisited*, 16 AM. REV. INT'L ARB. 177, 182–83 (2005) (discussing the differences in res judicata between common and civil law systems).

60. Davis v. U.S. Steel Supply, 688 F.2d 166, 171 (3d Cir. 1982).

61. *E.g.*, Amey, Inc. v. Gulf Abstract & Title, Inc., 758 F.2d 1486, 1509 (11th Cir. 1985).

62. Edward D. Cavanagh, *Issue Preclusion in Complex Litigation*, 29 REV. LITIG. 859, 868 (2010).

63. *E.g.*, Tofany v. NBS Imaging Sys., Inc., 616 N.E.2d 1034, 1037 (Ind. 1993) ("Generally, collateral estoppel operates to bar a subsequent re-litigation of the same fact or issue where that fact or issue was necessarily adjudicated in a former suit and the same fact or issue is presented in the subsequent lawsuit. In that situation, the first adjudication will be held conclusive even if the second is on a different claim.").

64. *E.g.*, New Hampshire v. Maine, 532 U.S. 742, 748–49 (2001). For instance, if Lee sues Mitchell in trespass and whether Mitchell has in fact trespassed is dependent on where Lee's property ends and Mitchell's begins, the adjudication of the property line is essential to the determination of Lee's cause of action. If Lee later cuts down trees on Mitchell's side of the boundary, Lee will be collaterally estopped in Mitchell's conversion suit from arguing the border. However, if Lee later sues Nolan in trespass after Nolan crossed onto Lee's land from Mitchell's, Nolan as a stranger to the initial litigation will not be collaterally estopped from arguing the border between Lee's and Mitchell's land. Likewise, a determination that was not essential to the verdict, such as the exact location of the border in parts of the property where there was no claim of trespass, would not be precluded from being relitigated in a subsequent proceeding.

65. *E.g.*, Comes v. Microsoft Corp., 709 N.W.2d 114, 121 (Iowa 2006). This may require a court to analyze the initial cause of action narrowly and to break a determination into its essential and non-essential elements. *E.g.*, A.B. Dick Co. v. Burroughs Corp., 713 F.2d 700, 704 (Fed. Cir. 1983) (refusing to give preclusive effect to a prior court's determination of the scope of a patent other than that court's determination as to its scope in regards to ink droplets due to non-essentiality).

Recognition of a foreign judgment is a prerequisite to res judicata of the cause of action and collateral estoppel as to any issue fully litigated on which the foreign judgment depended.[66] If the jurisdiction recognizes the award, it will generally find the cause of action or issue precluded if the cause of action or issue would be barred from being relitigated in the foreign jurisdiction that issued the judgment.[67] If, however, the issue would not be barred in the rendering jurisdiction, the court should not give it any preclusive effect.[68] Nonetheless, recognition of these judgments is vital, as non-recognition would render a court under the New York Convention unable to refuse recognition if the seat set aside the award, a ground that in and of itself is sufficient to refuse recognition.[69]

There appears to be no bar to recognizing a foreign judgment confirming, recognizing, or enforcing an arbitral award. Regardless of whether a court must use the common law or one of the uniform acts to reach recognition, the judgment should be cognizable. But an oddity may arise whereby a court would have to use certain legal principles to recognize a judgment confirming or recognizing an arbitral award, and different legal principles to recognize a judgment enforcing the award. Both of the uniform acts only apply to judgments granting or denying a recovery of money,[70] and although a comment to the 2005 version suggests the act applies to foreign judgments confirming arbitral awards,[71] mere confirmation does not appear to actually meet the definition of judgment inherent within it. This, in short, would make recognition of the judgment dependent on common law principles of foreign judgment law, while a judgment enforcing a foreign arbitral award—a judgment that in this situation has only theoretical distinction—could be enforced under a statutory scheme implemented by a state legislature. For example, Andrews may be told that Burnet owes him ten dollars—or Burnet may be told to pay Andrews ten dollars. It makes no sense to treat these situations differently. The legal relationship is the

66. *See* UNIF. FOREIGN-COUNTRY MONEY JUDGMENTS RECOGNITION ACT §4 cmt. 2 (2005) ("Recognition . . . has significance outside the enforcement context because a foreign-country judgment also must be recognized before it can be given preclusive effect under res judicata and collateral estoppel principles.").

67. *See, e.g.*, Phillips USA, Inc. v. Allflex USA, Inc., 77 F.3d 354, 360 (10th Cir. 1996) (determining that Kansas would look to Australian res judicata law to determine if a cause of action fully litigated on the merits in Australia would have res judicata effect in Australia before applying res judicata in Kansas); *cf.* Robert C. Casad, *Issue Preclusion and Foreign Country Judgments: Whose Law?*, 70 IOWA L. REV. 53, 75–76 (1984) (arguing that there is little justification in giving a foreign judgment greater preclusive effect in the United States than it would have in the rendering jurisdiction).

68. *See, e.g.*, Del. River Port Auth. v. Fraternal Order of Police, 290 F.3d 567, 573 (3d Cir. 2002) ("A federal court looks to the law of the adjudicating state to determine its preclusive effect."). Quite possibly the most common situation American courts are faced with is one in which federal courts have sole jurisdiction on a particular cause of action, but the parties have already litigated a parallel state claim in state court. In that situation, the federal court must look to state law to determine if state law would consider the state action as an estoppel to any related claim, even a claim that could not have been heard in the state court. *E.g.*, Marrese v. Am. Acad. of Orthopaedic Surgeons, 470 U.S. 373, 382–83 (1985).

69. New York Convention, *supra* note 12, art. V.1(e); *cf.* Giulia Carbone, *The Interference of the Court of the Seat with International Arbitration*, 2012 J. DISP. RESOL. 217, 220, 234 (comparing competing theories on the source of arbitration and what a judgment setting aside an award means under each theory).

70. *See supra* Part I.B.

71. UNIF. FOREIGN-COUNTRY MONEY JUDGMENTS RECOGNITION ACT § 2 cmt. 3 (2005) ("A judgment of a foreign court confirming or setting aside an arbitral award . . . would be covered by this Act.").

same, and the election or availability of one remedy over the other does not affect that relationship.

Although recognition is justified in both situations, it should be under common law principles. Recognition is an ancillary remedy, as the arbitral award itself contains the legally binding and enforceable rights, rights that have already been adjudicated under a legally adequate process.[72] Treating the foreign judgment as an independent primary remedy is inconsistent with viewing arbitration as an adequate dispute resolution system and subordinates arbitration to proper state-controlled judicial bodies. As discussed more fully *infra* Subparts III.A–B, while the judgment should be recognized, it should be done so as ancillary to enforcement of the arbitral award itself.

Thus, recognition is only half the battle. While judgments confirming, recognizing, or enforcing arbitral awards should be recognized as foreign judgments, the extent to which they deserve preclusive effect is debatable. I turn now to that issue.

III. ENFORCEMENT OF FOREIGN JUDGMENTS AND THEIR PRECLUSIVE VALUE

Recognition and enforcement are two distinct issues. While a court may recognize a foreign judgment, the extent to which it can give it effect depends in large part on the extent to which the judgment contains a determination of something enforceable under American law. This in turn requires an analysis of what cause of action the foreign court decided and which issues it addressed in coming to its judgment. The foreign judgment can be given effect as a money judgment for the amount of the award.[73] Or the foreign judgment can be given effect as an estoppel to an action to refuse recognition of the award.[74]

A. Merger and Parallel Entitlements

Two theories exist to give full effect to foreign judgments confirming, recognizing, or enforcing arbitral awards. The first, merger, treats the arbitral award as being merged into the judgment when the court in the primary jurisdiction confirms the validity of the underlying award.[75] Where merger operates, the award itself is unenforceable because the judgment has incorporated it, requiring enforcement of the judgment.[76] However, it seems that merger has not been adopted as a valid justification within the United States.[77] No doubt this is fortunate, as

72. *Cf.* Scherer, *supra* note 4, at 606 ("The ancillary nature of award judgments means that they relate to, and depend on, the prior adjudication in the award. They do not decide afresh the merits of the underlying dispute put before the arbitrators. Rather, award judgments focus on the validity of the award and its effects in the forum.").

73. *Infra* Part III.A.

74. *Infra* Part III.B.

75. *See, e.g.*, ALBERT JAN VAN DEN BERG, THE NEW YORK ARBITRATION CONVENTION OF 1958: TOWARDS A UNIFORM JUDICIAL INTERPRETATION 346–49 (1981) (discussing the merger theory)

76. *Id.*

77. *See, e.g.*, Island Territory of Curacao v. Solitron Devices, Inc., 489 F.2d 1313, 1323 (2d Cir. 1973)

merger would appear to be violative of the New York Convention.[78] If the award merges into the foreign judgment, the court will not be able to give recognition and enforcement to the award, thus avoiding the court's responsibilities under the Convention.

The other approach, parallel entitlements, has more support.[79] Under this theory, the award and the foreign judgment confirming the award create two separate avenues to collection; the party seeking enforcement can choose to enforce either at its discretion.[80] The Second Circuit—where the majority of attempts to enforce arbitral awards have taken place[81]—has given full effect to foreign judgments, allowing them to be enforced even if the underlying arbitral award could no longer be.[82] Other courts have not allowed enforcement of a foreign judgment as a workaround to enforcement of a limitations-barred arbitral award,[83] although these cases should not necessarily be read as a rejection of the parallel entitlements approach outside of a statute-of-limitations context.[84]

In the Second Circuit case of *Seetransport Wiking Trader v. Navimpex Centrala Navala*, the arbitral award was no longer enforceable, as the three-year statute of limitations for enforcement had run.[85] However, before enforcement was sought in the United States, Navimpex sought a set-aside of the award at the seat in France

(refusing to address whether the judgment of the court of Curacao merged into the arbitral award because the judgment was enforceable).

78. *Cf.* Scherer, *supra* note 4, at 601 (suggesting similar concerns).

79. The term "parallel entitlements" appears to have been coined in a textbook. TIBOR VÁRADY ET AL., INTERNATIONAL COMMERCIAL ARBITRATION: A TRANSNATIONAL PERSPECTIVE 688 (3d ed. 2006). The phrase was later used by a student note. Martin L. Roth, Note, *Recognition by Circumvention: Enforcing Foreign Arbitral Awards as Judgments*, 92 CORNELL L. REV. 573, 577–78 (2007). Both the phrase and the rationale behind the parallel entitlements approach have been adopted by the American Law Institute in its draft of the Restatement (Third) on the U.S. Law of International Commercial Arbitration. *See* RESTATEMENT (THIRD) OF THE U.S. LAW OF INT'L COMMERCIAL ARBITRATION § 4–3 reporters' note g (Council Draft No. 3, 2011) (adopting the parallel entitlements approach and name after listing cases that had followed it).

80. Scherer, *supra* note 4, at 601.

81. Roth, *supra* note 79, at 584.

82. *See* Seetransport Wiking Trader Schiffahrtsgellschaft MBH & Co., Kommanditgesellschaft v. Navimpex Centrala Navala, 29 F.3d 79, 83 (2d Cir. 1994) (affirming the District Court's enforcement of French judgment refusing to set aside arbitral award); *see also* Seetransport Wiking Trader Schiffahrtsgesellschaft MBH & Co., Kommanditgesellschaft v. Navimpex Centrala Navala (*Seetransport I*), 989 F.2d 572, 583 (2d Cir. 1993) (dismissing the cause of action to enforce the arbitral award due to statute of limitations but remanding to determine if French judgment confirming the award would still be enforceable in France); *cf. id.* at 586 (noting that Second Circuit cases "embody the parallel entitlements approach: the court may elect to recognize and enforce either the foreign arbitral award or the foreign confirmation judgment irrespective of the validity of the other claim").

83. *E.g.*, Comm'ns Imp. Exp. S.A. v. Republic of the Congo, 916 F. Supp. 2d 48, 57–58 (D.D.C. 2013). For an argument against enforcing a foreign judgment when the underlying arbitral award is barred by the applicable statute of limitations, see Roth, *supra* note 79, at 587–88.

84. The statute of limitations for enforcement of arbitral awards under the New York Convention is three years from the date the award becomes final. 9 U.S.C. § 207 (2012). The statute of limitations for the enforcement of foreign judgments varies from state to state. *Compare* WYO. STAT. ANN. § 1-3-105(a)(iii) (West 2014) (setting the statute of limitations at five years), *with* IDAHO CODE ANN. § 10-1409 (2010) (setting the statute of limitations at fifteen years unless the judgment would expire earlier in the rendering jurisdiction).

85. *Seetransport I*, 989 F.2d at 581.

and lost.[86] Yet because Seetransport did not seek enforcement in France, the French court did not order enforcement.[87] Thus, the Second Circuit remanded the case to the District Court to determine whether the judgment would be enforceable in France under French law, implying that if the judgment would be enforceable and collectable in France, it could be enforced and collected upon in the United States.[88] On remand, the District Court accepted evidence that when a French court dismisses a set-aside suit, it grants exequatur to the arbitral award, making the award enforceable within France.[89] The court therefore enforced the foreign judgment, making the award collectable in the United States.[90] The Second Circuit affirmed.[91]

On the most basic level, this approach ignores what the foreign judgment actually entailed. The enforcement or recognition action is, for all intents and purposes, a suit for ancillary relief. Under the New York Convention, the arbitration provides all the legally necessary adjudication to finally settle rights.[92] Assuming the arbitration and the agreement to submit to arbitration were legally sufficient, the court can never get to the merits of the dispute because there are no longer any merits left to be disputed. Like with a money damages judgment, the only remaining task is collection of the award. Yet when a party brings suit on the foreign judgment confirming, recognizing, or enforcing the arbitral award, the party is seeking ancillary relief for a judgment that was ancillary relief without ever pleading the existence of the dispute on the merits.[93] A cause of action based on an ancillary remedy cannot stand absent an underlying cause of action for which the ancillary relief is required.[94] Under such reasoning, courts have dismissed suits to appoint receivers—an ancillary remedy—absent an underlying claim either at law or in equity.[95] Likewise, it is error for a court to grant a preliminary injunction without the possibility of any other

86. *Id.* at 581–82.

87. *Id.* at 582.

88. *See id.* at 583 ("Herein, based upon the record before us, it is unclear whether the decision of the Court of Appeals of Paris, as it presently stands, is enforceable in France. Both parties have presented contradictory affidavits of French counsel, which have confused, rather than clarified the issue, and the district court has not addressed the issue.").

89. Seetransport Wiking Trader Schiffartgesellschaft, MBH & Co. v. Navimpex Centrala Navala, 837 F. Supp. 79, 80 (S.D.N.Y. 1993).

90. *Id.* at 81.

91. Seetransport Wiking Trader Schiffahrtsgesellschaft MBH & Co., Kommanditgesellschaft v. Navimpex Centrala Navala, 29 F.3d 79, 83 (2d Cir. 1994).

92. *See* New York Convention, *supra* note 12, art. III ("Each Contracting State shall recognize arbitral awards as binding and enforce them in accordance with the rules of procedure of the territory where the award is relied upon . . . .").

93. *Cf.* Scherer, *supra* note 4, at 606 ("The ancillary nature of [judgments confirming, recognizing, or enforcing an arbitral award] means that they relate to, and depend on, the prior adjudication in the award. They do not decide afresh the merits of the underlying dispute put before the arbitrators.").

94. *E.g.*, Fed. Sav. & Loan Ins. Corp. v. PSL Realty Co., 630 F.2d 515, 521 (7th Cir. 1980) (noting "the established rule" that a court lacks jurisdiction to grant ancillary relief in the absence of a substantive cause of action).

95. *E.g.*, Republic Trust Co. v. Taylor, 184 S.W. 772, 774 (Tex. Civ. App. 1916) ("It is well settled as a general rule that the appointment of receivers is an ancillary remedy in aid of the primary object of a litigation between the parties, and such relief must be germane to the principal suit; and a suit cannot be maintained under this general rule where the appointment of a receiver is the sole primary object of the suit, and no cause of action or ground for equitable relief otherwise is stated." (internal quotes omitted)).

litigation between the parties, as the preliminary injunction is an ancillary remedy to more permanent relief.[96]

Unless the award is treated as having merged into the foreign judgment, which no court in the United States has done,[97] or the party pleads the existence of the judgment for preclusive value while seeking enforcement of the award itself, the court lacks any non-ancillary controversy for which the ancillary relief is needed. The parallel entitlements approach thus is misguided; these judgments should be viewed as having no extraterritorial effect, as only being enforceable as an ancillary remedy in the national jurisdiction where rendered.[98] There is a judicial determination not of liability per se but merely that an arbitral award was valid under the laws of the state in which the *judgment* was made.

The better approach seems to be to only recognize the foreign judgments, thus allowing the judgments to have some level of preclusive effect. However, only the arbitral award itself should be capable of enforcement.

B. Preclusion

While enforcement of foreign judgments confirming, recognizing, or enforcing arbitral awards lacks any solid rationale, it does not follow that the foreign judgment serves no purpose. As the judgment can be recognized both under statutory law and common law principles,[99] it has the potential to be preclusive of certain claims and issues.[100] In this Subpart, I will first address whether the foreign judgment can result in the application of res judicata to claims of invalidity of the arbitral award. I will then address the foreign judgment's ability to collaterally estop issues litigated in the foreign court.

1. Res Judicata

The validity of using principles of res judicata in the context of enforcement of foreign judgments confirming, recognizing, or enforcing arbitral awards, at least in the United States, is so accepted as to not require comment in some judicial opinions.[101] However, the concept has been questioned and attacked from numerous

96. *See, e.g.*, Revelle v. Chamblee, 606 S.E.2d 712, 714 (N.C. Ct. App. 2005) (reversing a preliminary injunction where there were no other pending claims due to the preliminary injunction being an ancillary remedy).

97. *See supra* note 77 and accompanying text.

98. In her article on the issue, Dr. Scherer approaches this conclusion, but determines that because some issues are to be determined by a particular law, a decision by a court on that law is bound to have extraterritorial effect. Scherer, *supra* note 4, at 609–10. However, this both proves too much and not enough. It proves too much because it equates the issue of enforcement of the judgment with the preclusive effect particular issues within the judgment can have if the judgment is merely *recognized* by a different forum. These are two very different concerns in this context. Yet it also proves too little. While Dr. Scherer does address that judgments confirming arbitral awards are ancillary to the arbitral award itself, she fails to contextualize the significance of this outside the foreign judgment spectrum.

99. *Supra* Part I.B.

100. *Supra* note 51 and accompanying text.

101. *See, e.g.*, Belmont Partners, LLC v. Mina Mar Grp., Inc., 741 F. Supp. 2d 743, 750 (W.D. Va. 2010) (applying res judicata principles to a foreign judgment enforcing an arbitral award without

corners.[102] As I have already discussed, res judicata prevents the relitigation of a cause of action where the same parties fully litigated the action to a decision on the merits in a previous proceedings.[103] We can assume that the parties will be the same. Although the premise is shaky at best, for the sake of this Subpart we will assume that the previous judgment contained an adjudication on the merits and that that adjudication is final. Therefore, the question we must address is whether the cause of action in the U.S. court is essentially similar enough to bar the subsequent suit.

Some American courts have been hesitant to automatically apply res judicata when foreign judgments confirmed, recognized, or enforced arbitral awards. The Fifth Circuit has been the most hesitant, stating in dicta in *Karaha Bodas Co. v. Perusahaan Pertambangan Minyak Dan Gas Bumi Negara* that where the United States is a secondary jurisdiction under the New York Convention and a different secondary jurisdiction has issued a judgment, that judgment only enforces or refuses to enforce the award and should not automatically receive res judicata effect.[104] The Fifth Circuit recognized that "'relitigation' of issues is characteristic of the Convention's confirmation and enforcement scheme."[105] However, the relitigation is geographically limited, as the court in the secondary jurisdiction is only called upon to "enforce or refuse to enforce the foreign award, and then only within" the applicable secondary jurisdiction.[106]

Despite the Fifth Circuit's big-picture approach, other courts have been quick to pass off their decision-making authority to foreign courts. Quite possibly the most extreme example of a court giving res judicata effect occurred in *Belmont Partners, LLC v. Mina Mar Group, Inc.*, where the District Court for the Western District of Virginia found that res judicata barred Mina Mar's claims to set aside the award after a Canadian court upheld its validity.[107] Arbitration in the United States resulted in an award to Belmont Partners, which it successfully sought to enforce in Canada.[108] Belmont Partners later sought enforcement in the United States and argued res judicata against Mina Mar's defense of invalidity of the award.[109] The court found the causes of action sufficiently similar to warrant res judicata.[110] As it had in the proceedings in Canada, Mina Mar argued invalidity because the award was procured by fraud.[111] Thus, res judicata mandated the court grant comity to the Canadian court's determination that the award was not procured by fraud.[112]

---

addressing whether a judgment confirming an arbitral award merits a different analysis).

102. *E.g.*, Scherer, *supra* note 4, at 618 ("[I]f one were to grant preclusive effect to foreign recognition and enforcement judgments, this could only be done in a limited set of cases.").

103. *Supra* notes 56–61 and accompanying text.

104. 335 F.3d 357, 372 (5th Cir. 2003). The Second Circuit later agreed with the Fifth Circuit's general premise in subsequent litigation between the same two parties. Karaha Bodas Co. v. Perusahaan Pertambangan Minyak Dan Gas Bumi Negara, 500 F.3d 111, 123 (2d Cir. 2007).

105. *Karaha Bodas Co.*, 335 F.3d at 372.

106. *Id.* at 373.

107. Belmont Partners, LLC v. Mina Mar Grp., Inc., 741 F. Supp. 2d 743, 750–53 (W.D. Va. 2010).

108. *Id.* at 748–49.

109. *Id.* at 750.

110. *Id.* at 752–53.

111. *Id.* at 752.

112. *Id.* at 752–53.

But these courts miss the key issue of whether res judicata makes sense under any set of circumstances. Any issue not decided by the foreign court would make the judgment confirming, recognizing, or enforcing the award a different cause of action. A foreign award is enforceable unless one of seven conditions for non-enforcement is met. However, the cause of action for recognition (or setting aside) and enforcement of an arbitral award is explicitly individualized to the particular state where enforcement is sought. Article III of the New York Convention states that recognition within each contracting State leads to enforcement of the award "in accordance with the rules of procedure of the territory where the award is relied upon, under the conditions laid down in the following articles."[113] Article IV provides the conditions precedent to obtaining such recognition and enforcement.[114] And Article V, as already discussed, lays out the conditions under which a court may refuse to recognize and enforce a foreign arbitral award.[115] Yet this recognition and enforcement remains premised—as the Fifth Circuit correctly noted in *Karaha Bodas Co.*—on the fact that the particular State where the award is recognized and enforced has made these determinations. Belmont Partners cannot seek to determine the enforceability of the award in the United States in a proceeding in Canada, and a Canadian judgment cannot preclude litigation of the enforceability of the award in a foreign jurisdiction.

In *Belmont Partners*, for instance, this means that the Canadian court determined in a cause of action to enforce the award in Canada that the award was not the product of fraud. Even assuming that the definition of fraud is identical in both countries, a cause of action to recognize and enforce an award in Canada is a completely different cause of action than one to enforce an award in the United States, even if contrary to fact the seat was not in the United States. A cause of action to recognize and enforce an award is only determinative of the award's validity within the jurisdiction that renders the judgment. Even had Canada been the seat, an action to confirm an award only determines that the award is valid under the law of the primary jurisdiction, a different question from its recognition and enforceability in a secondary jurisdiction under the New York Convention. In *Belmont Partners*, this does not mean the issue of fraud must be relitigated; as will be discussed in the next Subpart, the *issue* could be collaterally estopped.[116] And since it was the only grounds through which Mina Mar challenged the award,[117] summary judgment could have been appropriate. Res judicata, however, is wholly inapplicable.[118]

---

113. New York Convention, *supra* note 12, art. III. Although the New York Convention does not define what is a "territory where an award is relied upon," it is well established that this is synonymous for the jurisdiction where enforcement is sought. *See, e.g.*, GARY BORN, INTERNATIONAL COMMERCIAL ARBITRATION 2913 (2d ed. 2014) ("[A]uthorities reach divergent conclusions on the question whether an award's preclusive effects are governed by the law of the arbitral seat (where the award was made) or the law of the recognition forum (where the award is relied upon).").

114. *See* New York Convention, *supra* note 12, art. IV (requiring a party to provide a certified copy of the award and if necessary a certified translation of the award in order "[t]o obtain the recognition and enforcement mentioned in [Article III]").

115. *Supra* notes 15–17 and accompanying text.

116. *See infra* Part III.B.2.

117. *Belmont Partners*, 741 F. Supp. 2d at 752–53.

118. This is not to say that res judicata cannot come up in the context of an arbitral award. It is well established that the award *itself* may be res judicata to any issues decided within the arbitration or claims

2. Collateral Estoppel

Collateral estoppel is a more interesting matter. Theoretically, if the parties fully litigated any of the seven grounds to refuse to recognize the award, such an issue could be precluded in U.S. courts, assuming of course that the foreign jurisdiction would also preclude relitigating the issue.[119] Likewise, if the parties fully litigated whether the award is valid under the law of the primary jurisdiction, issue preclusion could conceivably preclude such a determination from being relitigated.

Until now, I have not needed to differentiate between primary and secondary jurisdictions. The question of cognizability and enforceability of foreign judgments confirming arbitral awards did not invoke any such distinction; neither did the discussion on the possibility of the foreign judgment being res judicata to claims of invalidity of the award. Those issues could be resolved more generally, looking at the legal character of foreign judgments and res judicata. However, collateral estoppel is much more fact specific. An issue is precluded from relitigation because, under the facts of the previous adjudication, that *issue* was litigated and that *issue* was a necessary precondition of the ultimate judgment on the merits.[120] Such an issue can be either factual or legal (or somewhere in between).[121]

In this Subpart, I will first discuss what the difference is between primary and secondary jurisdiction and why it is significant. I will then discuss each of the grounds for refusing to recognize an arbitral award in a secondary jurisdiction to determine if any of them could be the grounds for issue preclusion within the secondary jurisdiction. Finally, I will move on to the issue of invalidity of the award under the law of the primary jurisdiction and the preclusive effects of such a determination.

---

that could have been raised in the arbitration. *E.g.*, Gulf Petro Trading Co. v. Nigerian Nat'l Petroleum Corp., 512 F.3d 742, 751–52 (5th Cir. 2008); *see also* George A. Bermann, *'Domesticating' the New York Convention: The Impact of the Federal Arbitration Act*, 2 J. INT'L DISP. SETTLEMENT 317, 323–24 (2011) ("The Restatement takes the position that judgments on [the scope of arbitration], whether rendered by a local or a foreign court, should be given the same preclusive effect that prior judgments generally enjoy under the forum's judgment recognition policies."). This is why the New York Convention allows for recognition and not just enforcement of arbitral awards. *See* FOUCHARD GALLIARD GOLDMAN ON INTERNATIONAL COMMERCIAL ARBITRATION § 1667 (Emmanuel Galliard & John Savage eds. 1999) ("In most cases, enforcement, not mere recognition, is sought. However, recognition may be requested where the party relying on an award merely wishes it to have a negative effect. In such a case, it is not easy to distinguish between recognition and the res judicata effect of arbitral awards." (footnote omitted)); *see also Gulf Petro*, 512 F.3d at 751–52 ("[T]he Convention acknowledges that foreign awards can serve as res judicata in secondary jurisdictions, and accordingly provides for the 'recognition' of an award, in addition to the more commonly invoked enforcement.").

119. *See supra* note 67 and accompanying text.

120. *E.g.*, Kroeger v. U.S. Postal Serv., 865 F.2d 235, 239 (Fed. Cir. 1988).

121. *E.g.*, Austin Wakeman Scott, *Collateral Estoppel by Judgment*, 56 HARV. L. REV. 1, 7 (1942) ("The doctrine of collateral estoppel is applicable not merely to questions of fact but also to questions of law.").

i. The Difference between Primary and Secondary Jurisdiction

Generally speaking, the primary jurisdiction is the seat of arbitration.[122] It is, under the parlance of the New York Convention, the place "in which, or under the law of which," a foreign arbitral award is made.[123] However, the seat need not be where the arbitration actually takes place.[124] As the Convention does not apply to recognition or enforcement of the arbitral award at the seat, the seat is not restricted to the enumerated grounds when deciding whether to set aside or confirm the award.[125] The seat and only the seat may look to its own law to determine if the award should be set aside.[126] Therefore, the primary jurisdiction has the "full range of [its] domestic law" to consider the award and determine whether to set it aside, modify it, or confirm it.[127] If the seat sets aside the award, courts in other jurisdictions may refuse to recognize and enforce the award for that very reason.[128]

Confirmation thus is only possible at the seat. On a technical level, there probably is no difference between saying a court confirmed an award and a court recognized an award.[129] However, on a more general level, it can be seen as the opposite of setting aside: If a court at the seat refuses to set aside an award, it has confirmed the award's validity.[130] It puts a word onto the particular and unique act a court at the seat does when it recognizes an award's validity. Thus, a judgment confirming an award may, under certain circumstances, not lead to any financial recovery. For instance, a party may not have any assets at the seat, yet because set aside is only possible in the primary jurisdiction, it may bring suit to set aside (or avoid the set aside of) the award. Therefore, despite the lack of a practical difference between the words confirmation and recognition, they serve the purpose of differentiating in kind between primary and secondary jurisdiction recognition.

---

122. *See, e.g.*, Rau, *supra* note 1, at 49 ("The 'seat' of the arbitration has been the fulcrum around which the entire arbitral enterprise pivots; in any discussion the fault line has been the supposed dichotomy between this state—where the arbitration finds its juridical 'home,' and whose jurisdiction over the process is therefore 'primary'—and all other states whose jurisdiction must therefore be deemed only 'secondary.'").

123. New York Convention, *supra* note 12, art. V.1(e).

124. *E.g.*, Rau, *supra* note 1, at 67–68 & n.45 ("[T]he arbitral 'seat' may be a 'pure fiction' . . . . For arbitrators may be forgiven if they should (understandably enough) prefer to dine in Paris rather than in Addis Ababa; the Court of Arbitration for Sport may understandably wish to develop a stable and unitary body of procedural law to govern its jurisprudence, even though the need for rapid on-site dispute resolution may require the evaluation of testimony in Sydney or Beijing." (footnote omitted)). Although beyond the scope of this Note, this author humbly disagrees with Professor Rau's assertion that it is understandable to prefer to dine in Paris than enjoy a hearty Ethiopian feast in Addis Ababa.

125. *See, e.g.*, Yusuf Ahmed Alghanim & Sons v. Toys "R" Us, Inc., 126 F.3d 15, 23 (2d Cir. 1997) (holding that the primary jurisdiction can set aside an award "in accordance with its domestic arbitral law" as well as any other grounds for relief available in that jurisdiction).

126. *E.g.*, VAN DEN BERG, *supra* note 75, at 350–51.

127. Gulf Petro Trading Co. v. Nigerian Nat'l Petroleum Corp., 512 F.3d 742, 747 (5th Cir. 2008).

128. New York Convention, *supra* note 12, art. V.1(e).

129. *But see* Scherer, *supra* note 4, at 590 (defining confirmation judgments as those "confirm[ing] that an award is valid and effective," and recognition judgments as those "decid[ing] on the validity of an award").

130. *See* Silberman & Scherer, *supra* note 11, at 330 n.81 (defining a "confirmation judgment" as a judgment that refuses to set aside an award).

Conversely, the secondary jurisdiction has limited jurisdiction under which to consider the award. It cannot be called upon to confirm (in the technical sense[131]) the award, and it cannot set aside the award.[132] Even the country whose substantive law governs the contract itself cannot set aside the award if that country is not the seat.[133] However, it (and any other secondary jurisdiction) may refuse to recognize or enforce the award for any reason specified in Article V of the Convention.[134]

Although this is just a cursory glance at the differences between primary and secondary jurisdiction, the difference in the scope of jurisdiction cannot be ignored as we turn to the effect a foreign judgment confirming, recognizing, or enforcing an arbitral award should have in a secondary jurisdiction.

ii. Secondary Jurisdiction Judgments

As a tribunal in a secondary jurisdiction can only refuse to recognize an arbitral award on a ground enumerated in the New York Convention, the grounds to refuse recognition of an arbitral award would appear to be the same regardless in which secondary jurisdiction enforcement is sought. However, this attempts to state too much. As I have already discussed, the Convention by its very terms only applies recognition locally.[135] But even if it did not, the question being asked—enforcement—is local to the secondary jurisdiction addressing the question. Many grounds for non-recognition are to be determined by local law of the secondary jurisdiction,[136] and even the public policy invoked[137] and the scope of applicability of

131. *See supra* note 11 (noting that confirmation occurs at the seat).

132. *See, e.g.*, M & C Corp. v. Erwin Behr GmbH & Co., KG, 87 F.3d 844, 849 (6th Cir. 1996) ("[A] motion to vacate may be heard only in the courts of the country where the arbitration occurred or in the courts of any country whose *procedural* law was specifically invoked in the contract calling for arbitration of contractual disputes."); *see also* Int'l Trading & Indus. Inv. Co. v. DynCorp Aerospace Tech., 763 F. Supp. 2d 12, 23–24 (D.D.C. 2011) (refusing to acknowledge judgment of Qatari court setting aside an award when the seat was Paris, yet the substantive law of the contract was Qatari law).

133. *E.g.*, Int'l Standard Elec. Corp. v. Bridas Sociedad Anonima Petrolera, Indus. y Comercial, 745 F. Supp. 172, 177–78 (S.D.N.Y. 1990). The *International Standard* court cited to cases from Belgium, France, India, South Africa, Spain, and West Germany in support of this proposition. *Id.* The New York Convention leaves open the possible interpretation that there can be more than one primary jurisdiction. Some scholars have proposed that if the law governing the contract is different from the law governing the arbitration, this other jurisdiction may be a primary jurisdiction able to set aside the award. *See* Karaha Bodas Co. v. Perusahaan Pertambangan Minyak Dan Gas Bumi Negara, 364 F.3d 274, 308–09 (5th Cir. 2004) (discussing the minority of authorities that interpret the New York Convention as allowing for two primary jurisdictions); *cf.* Catherine A. Giambastiani, *Recent Development:* Lex Loci Arbitri *and Annulment of Foreign Arbitral Awards in U.S. Courts*, 20 AM. U. INT'L L. REV. 1101, 1106–07 (2005) (citing to *Karaha Bodas* and discussing parties' ability to contract to change the primary jurisdiction). While there are scenarios by which this viewpoint may have validity—for example, if the law of the contract were a law that would not submit this sort of dispute to arbitration—we need not concern ourselves with those situations. In such situations, the award itself should be invalid under the law of the seat, as the parties would lack the ability to submit the dispute to arbitration no matter the *lex arbitri*.

134. New York Convention, *supra* note 12, art. V.

135. *Supra* notes 113–116 and accompanying text.

136. *Cf.* Mia Levi, *Inconsistent Application: Enforcing International Arbitral Awards in National Courts*, 27 N.Y. INT'L L. REV. 47, 62 (2014) ("As the local courts examine the arbitral awards, they inevitably input their own laws and norms onto the enforcement of such awards.").

137. *See, e.g.*, Bermann, *supra* note 118, at 331 (noting that, with respect to Article V of the Convention, the individual "US states are entitled to have and to enforce their own public policy" in

the Convention itself[138] are determined by the secondary jurisdiction's law in ratifying the Convention. A determination that an award violates public policy because the contract on which suit was brought was illegal in that jurisdiction should have no impact on the award's enforceability elsewhere, and especially not in a country that does not have the same public policy concern. Likewise, a determination that an award violates public policy in France because it gives punitive damages[139] contains the same localized determination that is inapplicable in countries with different legal concerns. However, this reasoning is insufficient to address whether the judgment should preclude litigation on whether the arbitral award is in fact illegal under that jurisdiction or awards punitive damages.

But other legal and policy concerns militate against granting any preclusive effect to secondary jurisdiction judgments. From a policy standpoint, as pertains to more general grounds to refuse recognition and enforcement, there is still an implicit judgment of the enforcing secondary forum that under its laws and its independent interpretation of its obligations under the New York Convention, the award is enforceable. Moreover, giving preclusive effect to these judgments would encourage parties to forum shop at the enforcement stage, seeking the jurisdiction most likely to uphold any alleged defects in the judgment.[140]

Furthermore, and most importantly, it overlooks that when an award debtor has assets spread globally, enforcement is frequently sought simultaneously in multiple forums.[141] It is not inconceivable that a party seeking non-recognition will dedicate more time and resources in the forums or forum where it has the most assets. Defeat in a forum where a party had less incentive to craft the strongest defense should not preclude relitigation in other jurisdictions. Returning to the punitive damages example, even the *fact* determined by the French court that the award granted a recovery of punitive damages suffers from these concerns, and that is assuming that what is legally defined as punitive damages is the same in France as it is in other jurisdictions. Even if it can be legally justified, it is unwise to grant any preclusive effect to recognition and enforcement judgments from secondary jurisdictions.

But policy concerns aside, the problem with giving preclusive effect to issues from secondary jurisdictions cannot be legally justified. Every ground in the New York Convention to refuse recognition of a foreign arbitral award is permissive.[142] A

---

refusing to recognize or enforce an award).

138. *See, e.g., id.* at 320 ("The Convention . . . permits ratifying States to declare themselves bound to recognize and enforce only those foreign awards rendered on the territory of another Contracting State.").

139. *See generally* Benjamin West Janke & François-Xavier Licari, *Enforcing Punitive Damage Awards in France after* Fountaine Pajot, 60 AM. J. COMP. L. 775 (2012).

140. *See* Scherer, *supra* note 4, at 611 (arguing that recognizing recognition judgments from secondary jurisdictions could encourage forum shopping).

141. *See id.* at 588 ("[T]he award creditor may initiate enforcement proceedings in countries in which the award debtor is believed to possess assets in order to collect the sums obtained in the award. . . . It is thus not uncommon to have judgments from different jurisdictions relating to the same award.").

142. *See supra* notes 21–22 and accompanying text; *see also* Jared Hanson, Note, *Setting Aside Public Policy: The* Pemex *Decision and the Case for Enforcing International Arbitral Awards Set Aside as Contrary to Public Policy*, 45 GEO. J. INT'L L. 825, 833 (2014) ("[While] the plain language of Article V of the New York Convention states that courts *may* refuse to recognize or enforce awards which have been set aside, it does not obligate them as it might have if it stated that courts *shall* refuse to enforce such awards.").

tribunal could in theory find reason to refuse to recognize the award on all seven enumerated grounds and still recognize the award. While of course no tribunal would in fact enforce an award that was against that nation's public policy, it is not unheard of for a tribunal to recognize an award despite the presence of a ground to refuse recognition. France, of course, has recognized and enforced foreign arbitral awards that had been set aside at the seat.[143] American courts have done so more infrequently.[144] Like the other six grounds, a set aside is sufficient to refuse recognition, but non-recognition cannot automatically follow.[145]

However, a judgment enforcing a foreign arbitral award has an even weaker basis. Such an award has not necessarily determined any fact other than that of the enforceability of the award within that jurisdiction. A determination in a secondary jurisdiction that the arbitration agreement was valid under the law of the seat cannot be necessary to the enforcement of the award, as the opposite determination—that the agreement was invalid—would not require the court to refuse recognition. Just the same, any fact that went into that judgment would also not be necessary to the judgment for the same reason. That each ground for non-recognition is not mandatory operates to prevent foreign judgments recognizing foreign arbitral awards from having any preclusive effect whatsoever. This thus requires a foreign tribunal to stay true to the New York Convention and enforce (or refuse to enforce) the award itself, not any ancillary foreign judgment.

iii. Primary Jurisdiction Judgments

Both theoretically and practically, there is more justification in giving foreign judgments confirming or enforcing arbitral awards from the primary jurisdiction preclusive value. Certain causes of action are only present in the proceedings in the primary jurisdiction, yet they can be determinative of important issues that are grounds for recognition or non-recognition of arbitral awards in secondary jurisdictions. Most obviously, New York Convention Article V.1(e) can only be applicable if a court in the primary jurisdiction has set aside the award.[146]

---

143. *See, e.g.*, Robert B. Kovacs, *Challenges to International Arbitral Awards: The French Approach*, 25 J. INT'L ARB. 421, 424 (2008) ("French case law . . . has been liberal in enforcing foreign arbitral awards under the [French procedural code], notwithstanding that an award has been set aside at the arbitral seat.").

144. There are only two reported cases where a United States district court has recognized an arbitral award that was set aside at the seat. *See generally* Corporación Mexicana de Mantenimiento Integral v. Pemex-Exploración y Producción, 962 F. Supp. 2d 642 (S.D.N.Y. 2013); *In re* Chromalloy Aeroservices, 939 F. Supp. 907 (D.D.C. 1996). The more recent case addressed the issue on remand from the Second Circuit after being asked to do so. *See* Corporación Mexicana de Mantenimiento Integral v. Pemex-Exploración y Producción, No. 10–4656–cv, 2012 WL 9346475, at *1 (2d Cir. Feb. 16, 2012) (remanding to address whether the order of a Mexican court setting aside the award should lead to the refusal to enforce the award in the district court).

145. *But see, e.g.*, Rau, *supra* note 1, at 84–85 (arguing that "while nothing in the Convention *requires*" a secondary jurisdiction to refuse to recognize an award set aside at the seat, the Convention nonetheless makes such deference "necessary and inevitable"); *cf.* Hanson, *supra* note 142, at 835 (arguing that the Federal Arbitration Act requires an American court to refuse to recognize or enforce an arbitral award that has been set aside at the seat).

146. *See* New York Convention, *supra* note 12, art. V.1(e) ("Recognition and enforcement of the award may be refused . . . [if t]he award . . . has been set aside or suspended by a competent authority of

Recognition of a judgment either setting aside or refusing to set aside the award must necessarily precondition this ground for non-recognition. While this is the justification for recognition of set-aside judgments, a confirmation or enforcement judgment can serve other preclusive purposes. If in confirming an award the primary jurisdiction determines that the arbitration agreement was valid under its law, this should collaterally estop the contestant from relitigating in a secondary jurisdiction invalidity of the agreement under seat law.[147] This issue, which was necessary for the determination that the arbitration and award are valid under the law of the seat, has been determined, and any fact that necessarily contributed to this determination should be considered as established when enforcement is sought in the secondary jurisdiction.

However, courts must be careful at this stage to separate determinations that the arbitral award is valid under primary jurisdiction law from determinations that the secondary jurisdiction should have the requirement of recognizing the award in the first instance when faced with a suit for recognition and enforcement of the award. For instance, a determination that the requirement under primary jurisdiction law that a party have notice before being bound by an arbitral award is not and cannot be preclusive of the fact that the notice was adequate to give cognizance to the award within the secondary jurisdiction. The issue in the confirmation judgment—notice under primary jurisdiction law—is still different than the issue in the secondary jurisdiction of whether that notice meets the definition of notice under the law of the secondary jurisdiction. The substitution of one issue for a different one prevents the secondary jurisdiction court from relying on the foreign judgment on that issue.

But this limitation should not prevent an underlying fact from being collaterally estopped. To use the notice example, a determination of the fact that a party mailed the summons by return receipt requested mail and that the recipient did in fact sign for the summons should preclude relitigation of that fact in a secondary jurisdiction. The same concerns that require no preclusive effect if that fact was determined by a court of secondary jurisdiction are absent when the judgment comes from a primary jurisdiction. Even if a party does not have assets in the primary jurisdiction, the party still has unsurpassed incentive to litigate the award's invalidity in the proceedings in the primary jurisdiction. That is, almost all jurisdictions and scholars agree that an award set aside at the seat is unenforceable elsewhere.[148] And unlike in a proceeding in a secondary jurisdiction, the party challenging the award is not limited to challenging on the few grounds listed in the New York Convention.[149] Thus, there are not the same concerns about forum shopping or litigation incentives as there are when a party seeks enforcement in a secondary jurisdiction. So long as the fact determined was necessary for confirming the award's validity at the seat, that fact should be collaterally estopped in a future suit in a secondary jurisdiction.

---

the country in which, or under the law of which, that award was made.").

147. *See id.* art. V:1(a) ("Recognition and enforcement of the award may be refused . . . [if] the said agreement is not valid under the law to which the parties have subjected it . . . .").

148. *See, e.g.*, Rau, *supra* note 1, at 83–85 (arguing that annulment at the seat should render the award unenforceable globally).

149. *See supra* note 12 and accompanying text.

CONCLUSION

The misconception U.S. courts have of foreign judgments confirming, recognizing, and enforcing arbitral awards is not surprising when you consider the procedural nature of the judgment. The significance of ancillary remedies is easily overlooked, and a court with limited resources will not be wont to take on the often difficult task of analyzing both a foreign judgment and an underlying arbitral award when a court of competent jurisdiction has previously fully done one of these tasks. Likewise, the small distinction that a court can recognize a judgment without enforcing it can easily be overlooked, especially where the judgment cannot be enforced because there is nothing to enforce.

However, by contextualizing the foreign judgment as an ancillary remedy to enforcement of the arbitral award, and by acknowledging that recognizing the foreign judgment can collaterally estop a party from relitigating certain issues that the foreign judgment was based on, a U.S. court can both conserve its resources and uphold the United States' duty under the New York Convention to recognize and enforce arbitral awards rendered in a foreign country. But a court must be careful. For both legal reasons under the New York Convention and policy reasons, it should limit preclusion only to those legal issues that relate to the award's validity under the law of the primary jurisdiction, and even then only if such a determination was made in the primary jurisdiction itself. And a court should only grant preclusive effect to facts if those facts were determined by the primary jurisdiction in making the determination of the award's validity under the law of that jurisdiction. Otherwise, the court should consider everything afresh, determining for itself whether the award merits recognition and enforcement.

Achieving Universalism in MEG Insolvencies: An Analysis of Whether the German Stock Corporation Act of 1965 Could Help

MEGHAN WIED*

TABLE OF CONTENTS

* Meghan Wied, J.D., the University of Texas School of Law 2015.

INTRODUCTION & OVERVIEW

This Note attempts to study the problem of creditor uncertainty in insolvency proceedings caused by the various ways the corporate form can be disregarded internationally in the context of multinational enterprise groups (MEGs), and the solutions available to treat that problem. It is divided into four major parts.

First, in Part I, the Note presents the problem. It illustrates, through the examination of laws within a single jurisdiction and the introduction of multinational bankruptcy, the unpredictability faced by creditors of MEGs within existing legal regimes. Although the widespread approach is to respect the corporate form, jurisdictions can and do subject entities to "intra-group" liability, thereby consolidating, in whole or in part, the entities' assets.

Next, in Part II, the Note discusses the various insolvency goals to be achieved in the insolvency of MEGs, namely the maximum preservation of assets, procedural coordination, fairness, and predictability. With these goals in mind, multinational and entity versus enterprise group-specific considerations are discussed in order to frame the context in which the methods to attain these goals have to be considered.

Putting these two concepts together, Part III of the Note seeks to explain the progress that has been made in this field by the U.N. Commission on International Trade Law (UNCITRAL) and analyzes whether the German Stock Corporation Act of 1965 could be a good starting place for a model law in this area. Although it has not addressed MEGs in insolvency with a model law, UNCITRAL has offered some legislative guidance in terms of the procedural coordination of MEG insolvencies via cooperation. However, more could be done in terms of achieving predictability. This Note next analyzes Germany's innovative legislative approach to enterprise liability to see if it could be a good working model.

In conclusion, this Note surmises that the German Stock Corporation Act of 1965 could be a good starting place for a UNCITRAL model law for four significant reasons: It could reduce litigation, it is capable of regulating diverse enterprise groups, it provides a balanced approach to liability, and it reframes the discussion of enterprise liability in permissive terms. However, such a model law needs to be modified in several respects.

I. THE PROBLEM – ADAPTING THE LAW TO MULTINATIONAL ENTERPRISE GROUPS, MAINTAINING ASSET SECURITY, & MEETING CREDITOR EXPECTATIONS IN BANKRUPTCY

A. Generally

Today we live in a world that is constantly evolving and interconnected, where corporations have branches across the globe. Behind us are the days dominated by mom-and-pop stores, operations with one establishment, operations within one state, or even operations only within one country by individual shareholders or owners.[1] In fact, according to the 2009 World Investment Report published by the U.N. Commission on Trade and Development, there are some 82,000 MEGs worldwide, with 810,000 foreign affiliates in the world.[2] Despite this, the law on corporate groups globally remains ever stable—shielding individuals from liability and segregating assets of what are considered "distinct entities."[3] But, in this integrated world, particularly with respect to multinational groups, does this still make sense? And if in some cases it doesn't, how should the international community cope with multinational exceptions to the rule? As an initial point, it is important to note that many commentators argue that entity analysis is not appropriate for highly integrated MEGs;[4] however, even if one disagrees with this argument, the fact remains that jurisdictions are full of creative and varied ways to get around the problem of separate corporate personalities.[5]

Problems related to the treatment of entities within MEGs as separate personalities arise in many different contexts: personal injury, environmental regulation, taxes, and disclosure, among others. As one commentator has noted, "[i]n probably no other area has enterprise law received more general acceptance

---

1. *See* Irit Mevorach, *Towards a Consensus on the Treatment of Multinational Enterprise Groups in Insolvency*, 18 CARDOZO J. INT'L & COMP. L. 359, 361–62 (2010) [hereinafter Mevorach, *Towards a Consensus*] ("Multinational enterprise groups (MEGs), namely businesses comprised of separate entities which operate in more than one country, dominate the global commercial world." (footnote omitted)).

2. U.N. CONFERENCE ON TRADE & DEV., WORLD INVESTMENT REPORT: TRANSNATIONAL CORPORATIONS, AGRICULTURAL PRODUCTION AND DEVELOPMENT, at 17, U.N. Sales No. E.09.II.D.15 (2009), *available at* http://unctad.org/en/Docs/wir2009_en.pdf.

3. Irit Mevorach, *Is the Future Bright for Enterprise Groups in Insolvency? An Analysis of UNCITRAL's New Recommendations*, *in* INTERNATIONAL INSOLVENCY LAW: REFORMS AND CHALLENGES 363, 369 (Paul Omar ed., 2013) [hereinafter Mevorach, *Is the Future Bright*] ("Generally, legal systems tend to adhere to the concept of the corporate form permitting separate personality and limited liability to be the default rules for companies even in respect to the relationship between companies and their 'sisters' or 'parents' in a group context.").

4. PHILLIP I. BLUMBERG, THE MULTINATIONAL CHALLENGE TO CORPORATION LAW: THE SEARCH FOR A NEW CORPORATE PERSONALITY 232 (1993) [hereinafter BLUMBERG, MULTINATIONAL CHALLENGE] ("The concept of the corporation as a separate legal entity, a concept that originally had satisfactorily defined the economic entity as well as the legal entity, has failed to correspond to the modern realities of American and world business. Early nineteenth-century law no longer serves the legal needs of the late twentieth-century economic order." (footnote omitted)).

5. *See* Anthony V. Sexton, *Current Problems and Trends in the Administration of Transnational Insolvencies Involving Enterprise Groups: The Mixed Record of Protocols, the UNCITRAL Model Insolvency Law, and the EU Insolvency Regulation*, 12 CHI. J. INT'L L. 811, 832 (2012) (contrasting how the European Union treats related entities to how the United States does).

than in the area of disclosure."[6] In the case of insolvency, how separate entities are viewed—separately or as a group—is very important in determining entity liability and asset allocation that matches or disrupts creditors' expectations.[7] Inevitably, the separate contexts in which the enterprise-entity problem arises backdoor their way into an insolvency, depending on the way the assets are parsed.[8] However, the focus of this Note is on ignoring the corporate form more generally when creditors of one entity try to reach the assets of another that is close to insolvency via intragroup claims.

Below are two brief examples of some of the complexities and issues that arise in this area. The hope is that after reading these examples, a reader will be able to imagine the immeasurable amount of uncertainty that creditors currently face in the case of cross-border insolvency of MEGs, particularly with respect to when the corporate entity will be disregarded and its assets, in whole or in part, merged with another entity.

B. Single Jurisdictions

Even within single jurisdictions, whether a corporate entity's assets will remain separate is uncertain. In the United States, for example, the Third Circuit has recognized that multiple theories exist for ignoring the corporate form.[9] Among others, these include: piercing the corporate veil, equitable subordination, remedies for turnover and fraudulent transfer pricing, and substantive consolidation.[10]

As one scholar has noted, piercing the corporate veil is one of the "most litigated issue[s] in corporate law and yet it remains among the least understood."[11] In general, piercing the corporate veil is a term used to describe instances when a court decides to ignore the corporate form and hold shareholders liable for the actions of the corporation.[12] In applying the doctrine, U.S. courts have cited a number of reasons to disregard the corporate form, with each court usually applying more than one.[13] A sampling of these reasons include undercapitalization; failure to

6. BLUMBERG, MULTINATIONAL CHALLENGE, *supra* note 4, at 196.

7. *See* John H. Matheson, *The Modern Law of Corporate Groups: An Empirical Study of Piercing the Corporate Veil in the Parent-Subsidiary Context*, 87 N.C. L. REV. 1091, 1094–95 (2009) ("One particular application of the law of corporate groups entails dealing with the ramifications of subsidiary insolvency. Global competition, product and management failures, economic fluctuations, government regulation, tort claims, and environmental cleanups are just some of the circumstances and events that may imperil the financial life of a subsidiary company. When a subsidiary corporation is subject to significant unsatisfied claims or impending bankruptcy, claimants may call upon the courts to exercise traditional equitable powers to ignore the legal separateness of the subsidiary and to hold the parent company liable for the subsidiary's debts.").

8. *Cf.* Allan L. Gropper, *The Payment of Priority Claims in Cross-Border Insolvency Cases*, 46 TEX. INT'L L.J. 559, 562 (2011) ("[M]ost multinational enterprises are organized in separate business units, whether as corporations or limited liability companies, in the different jurisdictions in which they operate. This structure may not owe its genesis to insolvency issues but to tax or corporate governance concerns; however, it still has important implications in the event of the failure of the enterprise.").

9. *In re* Owens Corning, 419 F.3d 195, 206 (3d Cir. 2005).

10. *Id.* Although these remedies have subtle differences, they all result in corporate disregard. *Id.*

11. Robert B. Thompson, *Piercing the Corporate Veil: An Empirical Study*, 76 CORNELL L. REV. 1036, 1036 (1991) (footnote omitted).

12. *Id.*

13. *Id.* at 1044–45.

follow corporate formalities; overlap of economic records, functions, or personnel; misrepresentation; shareholder domination; use of the corporation as an "alter ego" or instrumentality; fairness; assumption of risk; and statutory policy.[14] In all, the reasons to pierce the corporate veil tend to be supported by the notion that the legal entity has been "used to defeat public convenience, justify wrong, protect fraud, or defend crime,"[15] and the decisions reached by the courts have been perceived to be fair and correct;[16] however, it is generally recognized that the case law with respect to piercing the corporate veil is "irreconcilable and not entirely comprehensible."[17]

Alternatively, equitable subordination may place "bad-acting creditors behind other creditors when distributions are made."[18] In terms of a parent-subsidiary or sister-subsidiary relationship, equitable subordination is likely to happen when "a corporate parent [or sister subsidiary] is both a creditor of a subsidiary and so dominates the affairs of that [subsidiary] as to prejudice unfairly its other creditors."[19] Basically, equitable subordination subjects intragroup claims to special scrutiny and evaluates them "according to equitable principles governing conduct by fiduciaries. [To avoid this result, t]he parent corporation or other insider must demonstrate not only the fairness of the intercompany transaction giving rise to the claim, but the fairness of its other interrelationships with the subsidiary (or controlled corporation) as well."[20]

Similarly, but more drastically, remedies for turnover and fraudulent transfers may "bring back to the transferor debtor assets improperly transferred to another (often an affiliate)."[21] To make a prima facie case of a fraudulent transfer under the U.S. Bankruptcy Code, one must prove that a person incurred an obligation or transfer of an interest of the debtor within two years of the bankruptcy for which the debtor received less than reasonably equivalent value; moreover, this transaction must have occurred while the debtor was either insolvent, left with unreasonably small capital, incurred debts beyond the debtor's ability to pay, or made a transfer to or for the benefit of an insider under employment.[22] If the party is successful in proving such a case and no defense applies, the prevailing party may avoid the fraudulent transfer and recover either the property or the value of the property transferred plus interest.[23]

---

14. *Id.* (listing the major categories of reasons courts gave for piercing the corporate veil in the 1600 cases the author studied).

15. *Id.* at 1041 (quoting United States v. Milwaukee Refrigerator Transit Co., 142 F. 247, 255 (C.C.E.D. Wis. 1905) (internal quotation marks omitted).

16. *Id.* at 1037 ("[M]any believe . . . courts are getting it right. An early scholar in this area, Elvin Latty, observed that, 'in spite of conflicting and misleading dicta the judicial hunch usually carries through to a correct decision.'" (quoting Elvin R. Latty, *The Corporate Entity as a Solvent of Legal Problems*, 34 MICH. L. REV. 597, 630 (1936))).

17. PHILLIP I. BLUMBERG, THE LAW OF CORPORATE GROUPS: PROCEDURAL PROBLEMS IN THE LAW OF PARENT AND SUBSIDIARY CORPORATIONS 8 (1983).

18. *In re* Owens Corning, 419 F.3d 195, 206 (3d Cir. 2005).

19. *Id.*

20. BLUMBERG, MULTINATIONAL CHALLENGE, *supra* note 4, at 118.

21. *Owens Corning*, 419 F.3d at 206.

22. 11 U.S.C. § 548(a)(1)(B)(i)–(ii) (2012); *accord* DAVID M. HOLLIDAY, CAUSE OF ACTION IN BANKRUPTCY CASE FOR AVOIDANCE OF PREPETITION FRAUDULENT TRANSFER OR OBLIGATION UNDER 11 U.S.C.A. § 548(A)(1)(B), 39 CAUSES OF ACTION §§ 5–13 (2d ed. 2009).

23. HOLLIDAY, *supra* note 22, §§ 61–63 (discussing remedies and relief).

Also, in a turnover proceeding, the ownership of property is not in dispute; rather, the proceeding is used as a "remedy to obtain what is acknowledged to be property of a debtor's estate."[24] In the context of enterprise groups, turnover proceedings may be considered an ancestor of substantive consolidation, which will be discussed next.[25]

Finally, in the context of bankruptcy specifically, a corporation's separate legal existence may be ignored via substantive consolidation. Substantive consolidation "brings all the assets [and liabilities] of a group of entities [together] into a single survivor."[26] Although it is rarely invoked, there is a variety of reasons for substantive consolidation, and its effects are drastic.[27] Among the reasons are: (1) one entity is the alter ego of another, through the doctrine of "pierc[ing]-the-corporate-veil"; (2) the negative practical effects of parsing through the "tangled affairs of entities, separate in name only," is so great that it would be simpler to consolidate; and (3) similarly, the accounting is so complex that some information, necessary to right an inequity, is untraceable.[28] As a result of substantive consolidation, "claims of creditors against separate debtors morph [in]to claims against the consolidated survivor."[29] The net effect is that post hoc two entities, once separated, are treated as a single enterprise regardless of the expectations of the separate entity's creditors. If that is not scary enough, consider that it is not a threat without bite—in the years 2000–2004 alone, eleven of the twenty-one largest bankruptcies, measured by asset value prior to filing, used substantive consolidation, and three reserved the right to use it in the future.[30]

Overall, these various remedies have the potential to effectuate the same result: to consolidate, either partially or in whole, the assets of various "group" members, whether through liability or convenience.[31] Although it is conceded that each of these might serve a slightly different function, they are all remedies aimed at preventing the "abuse" of the corporate form;[32] the problem is, from a creditor's perspective, how and when these various doctrines will be used is unpredictable.

---

24. Marlow v. Oakland Gin Co. (*In re* Julien Co.), 128 B.R. 987, 993 (Bankr. W.D. Tenn. 1991), *aff'd*, 44 F.3d 426 (6th Cir. 1995).

25. Mary Elisabeth Kors, *Altered Egos: Deciphering Substantive Consolidation*, 59 U. PITT. L. REV. 381, 389 (1998).

26. *Owens Corning*, 419 F.3d at 206.

27. *Compare id.* at 208–09 ("[T]here appears nearly unanimous consensus that [substantive consolidation] is a remedy to be used 'sparingly.'"), *with* William H. Widen, *Corporate Form and Substantive Consolidation*, 75 GEO. WASH. L. REV. 237, 252 (2007) ("My preliminary empirical study of the twenty-one largest corporate bankruptcy filings from 2000 to 2004, ranked by asset size, reveals that substantive consolidation was imposed, proposed, or settled in eleven of those cases.").

28. *Owens Corning*, 419 F.3d at 207.

29. Genesis Health Ventures, Inc. v. Stapleton (*In re* Genesis Health Ventures, Inc.), 402 F.3d 416, 423 (3d Cir. 2005).

30. William H. Widen, *Prevalence of Substantive Consolidation in Large Bankruptcies from 2000 to 2004: Preliminary Results*, 14 AM. BANKR. INST. L. REV. 47, 53 (2006). Most notably, these bankruptcies included giants such as Enron, WorldCom, United Airlines, and PG&E Energy Group. *Id.* at 59.

31. Judith Elkin, *Lifting the Veil and Finding the Pot of Gold: Piercing the Corporate Veil and Substantive Consolidation in the United States*, 6 DISP. RESOL. INT'L. 131, 131–32 (2012).

32. *E.g.*, LFC Mktg. Grp., Inc. v. Loomis, 8 P.3d 841, 845–46 (Nev. 2000) ("[T]he essence of the alter ego doctrine is to 'do justice' whenever it appears that the protections provided by the corporate form are being abused.").

C. *Multiple Jurisdictions*

Projecting single jurisdiction uncertainty onto the multinational stage, it becomes apparent that this topic is ripe for consideration. Consider, for example, the recent bankruptcy and restructuring of Nortel Networks.[33] Nortel Networks is a global communications corporation that initially started in Canada manufacturing and supplying equipment for the telecommunications industry.[34] As technology developed, Nortel Networks got more involved with satellite equipment, fiber optics, and cellular phones.[35] Simultaneously, Nortel also expanded globally.[36]

For over one hundred years, Nortel's business was highly successful, but like many other technology companies in the late 1990s and early 2000s, Nortel began to experience financial trouble.[37] In January of 2009, "Nortel initiated creditor protection proceedings in multiple jurisdictions."[38] Across these jurisdictions, courts were presented with the challenge of how to allocate and distribute the billions of dollars worth of salvaged assets among the related entities.[39] As a part of these proceedings in the United States, the United States Bankruptcy Court for the District of Delaware found itself presented with a motion to dismiss the claims of three foreign sister subsidiaries against the principal U.S. operating subsidiary of the Canadian parent of Nortel.[40] The motion amounted to a claim that the U.S. subsidiary "improperly diverted or assisted in diverting cash and value from them for the benefit of . . . the Canadian parent company."[41] These claims ran the gamut from alleging that the U.S. subsidiary had breached its fiduciary duties, aided and abetted the breach of fiduciary duties, committed a civil conspiracy, and unjustly enriched its creditors to claims that the U.S. subsidiary should have its creditor claims subrogated; the foreign subsidiaries forced the Delaware bankruptcy court to apply American civil procedure concepts to measure claims derived from English, Irish, and French substantive law.[42] It seems unlikely that creditors of the American subsidiary would have anticipated having their already small reparations reduced even further by claims of foreign sister subsidiaries, but many of the claims proceeded anyway.

As part of the ongoing bankruptcy proceeding, many of these U.S. claims were ultimately settled in early 2014, although some cross-border claims remain.[43] But in

---

33. *About Us*, NORTEL NETWORKS CORP., http://www.nortel-canada.com/about/ (last visited June 15, 2015).

34. *History of Nortel*, NORTEL NETWORKS CORP., http://www.nortel-canada.com/about/history/ (last visited June 15, 2015).

35. *Id.*

36. *1970 to 1999*, NORTEL NETWORKS CORP., http://www.nortel-canada.com/about/history/1970-to-1999/ (last visited June 15, 2015).

37. *See* Sean Michael Kerner, *Nortel Bankruptcy a Canadian Tragedy*, INTERNET NEWS (Jan. 16, 2009), http://www.internetnews.com/commentary/article.php/3796971/Nortel+Bankruptcy+a+Canadian+Tragedy.htm (explaining that Nortel's decline coincided with the dot-com bubble).

38. *Welcome*, NORTEL NETWORKS CORP., http://www.nortel-canada.com/ (last visited June 15, 2015).

39. *E.g.*, *In re* Nortel Networks, Inc., 469 B.R. 478, 485 (Bankr. D. Del. 2012).

40. *Id.*

41. *Id.*

42. *See id.* at 498–518 (listing and analyzing the various claims under foreign and U.S. law).

43. *Compare* Tom Hals, *'Milestone' Nortel Settlement Gets Court Approval*, REUTERS, Jan. 7, 2014,

examining this case, one thing becomes clear: Although "[r]espect [for] the corporate form is a widespread approach,"[44] corporate separateness and limited liability are not "absolute."[45] Multiple jurisdictions have ways of ignoring the corporate form, or finding "intra-group" liability.[46] Because entities are not subject to enterprise liability, these types of mechanisms—"intra-group" claims—provided by statute or case law represent some of the only equitable options to increase the assets of an insolvent entity when it has possibly been used to its detriment by another entity.[47] The problem in a multinational context is that these types of claims vary,[48] which drags out litigation[49] and produces uncertainty for creditors of entities that operate under or within an "enterprise group."

To date, as the claims articulated above exhibit, the emphasis for ignoring the corporate form and commingling assets has been on wrongdoing and has failed to come to terms with "the realities of the modern concepts of [MEGs]."[50] Moving forward, enterprise law could address some of the current legal inadequacies "if it encompassed the normal, rather than the exceptional, considerations of [MEG] economic activity," and "evade[d] the requisite for 'inequitable' or 'morally culpable' conduct to exist between a parent and subsidiary company."[51]

---

available at http://www.reuters.com/article/2014/01/07/nortel-bankruptcy-settlement-idUSL2N0KH1KN20140107 (announcing court approval of the settlement of claims in U.S. court from European investors), *with* Tom Hals, *Nortel Networks to Pay U.S. Bondholders Up to $1 Bln in Interest*, REUTERS, July 24, 2014, *available at* http://www.reuters.com/article/2014/07/25/nortel-bankruptcy-idUSL4N0PZ7CA20140725 (discussing the effects of a proposed settlement on remaining claims).

44. Mevorach, *Towards a Consensus*, *supra* note 1, at 376.

45. *See id.* (addressing limitations to aspects of the corporate form).

46. *See* BLUMBERG, MULTINATIONAL CHALLENGE, *supra* note 4, at 92–96 (discussing how various common law courts have expanded the avenues to ignore corporate protections).

47. *See* Matheson, *supra* note 7, at 1095–97 ("Given the massive financial assets of many multinational parent corporations, actions seeking to ignore the legal separateness of a corporate subsidiary of a parent company offer some of the biggest potential payoffs for claimants.... [There is] considerable impact of U.S. common law on foreign legal systems, many of which draw heavily from American concepts and court decisions.").

48. *See* IRIT MEVORACH, INSOLVENCY WITHIN MULTINATIONAL ENTERPRISE GROUPS 55 (2009) [hereinafter MEVORACH, INSOLVENCY WITHIN MEGs] ("[T]he degree to which any exceptions to limited liability can be grounded on group considerations... is largely uncertain and varies among legal systems.").

49. *See* Nora Wouters & Alla Raykin, *Corporate Group Cross-Border Insolvencies between the United States & European Union: Legal & Economic Developments*, 29 EMORY BANKR. DEV. J. 387, 397 (2013) (discussing the Nortel insolvency and noting that despite its universalist success in sale after sale, "there were still disputes between the different affiliates with competing interests" that resulted in litigation across countries).

50. Muzaffer Eroglu, Modern Organisation of Multinational Enterprises And Liability Discussions: Critical Analysis Of Control Theory 1–2 (Dec. 23, 2008), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1319733.

51. *See* Binda Sahni, *The Interpretation of the Corporate Personality of Transnational Corporations*, 15 WIDENER L.J. 1, 38 (2005) (addressing the more narrow topic of fashioning enterprise liability to cover involuntary creditors, such as tort claimants).

II. THE GOAL – MEETING CREDITORS' EXPECTATIONS WHILE SIMULTANEOUSLY CONTINUING TO STIMULATE GLOBAL INNOVATION AND COOPERATION

In crafting a remedy to address the problem of creditor uncertainty relating to the treatment of MEGs, it is important to consider the goals of the various parties who have a stake in an insolvency proceeding. "Generally, insolvency laws will be aimed at enhancing wealth maximization, . . . respect[ing] pre-entitlements of creditors and promot[ing] certainty, as well as wider goals, in particular equitable treatment of creditors, procedural fairness and facilitation of rescues."[52] In trying to match these goals, however, a number of factors distinct to enterprise group insolvency in the multinational context must be considered: how to balance limited liability with economic realities, how to coordinate proceedings across jurisdictions, and what result will best match competing creditors' expectations.

A. Balancing Limited Liability with Economic Realities

Even with the aspirational goal of trying to harmonize MEG insolvency law to match economic realities, it is important to keep in mind, with respect to limited liability, that you cannot throw the baby out with the bath water. There is a real tension between the need for limited liability provided by separate entities and the economic advantages that come with group integration. Limited liability, for example, has been revered for a number of perceived advantages: "(a) encouraging investment without participation in control, . . . thereby promoting large-scale investment and corporate activity; (b) promoting the efficiency of the capital markets; (c) avoiding the allegedly intolerable inefficiencies of a liability system; and (d) stimulating entrepreneurial risk-taking and risk diversification."[53] As such, even proponents of enterprise concepts agree that "[t]he promotion of insolvency goals should not undermine the limited liability concept, unless enterprise law points to a factual circumstance where limited liability and 'asset partitioning' were not kept in terms of economic reality (where there was no partitioning in the ordinary course of business)."[54]

At the same time, corporate separateness in the enterprise group context has been criticized because the above rationales do not seem to apply with as much force when the parent company is the shareholder, particularly one conducting a common business across the enterprise.[55] Related to this issue is that limited liability "may create the possibility of externalization of some costs of the enterprise with risk falling on outsiders."[56]

52. Mevorach, *Is the Future Bright*, *supra* note 3, at 368.
53. BLUMBERG, MULTINATIONAL CHALLENGE, *supra* note 4, at 125.
54. Mevorach, *Is the Future Bright*, *supra* note 3, at 373.
55. *E.g.*, MEVORACH, INSOLVENCY WITHIN MEGS, *supra* note 48, at 42–43.
56. *Id.* at 44.

B. Coordinating Proceedings

Along the same lines, as an intermediate and separate matter, even if a person is unwilling to sacrifice limited liability for more predictability when group assets will be integrated, most can agree that proceedings should be coordinated such that the group's return on assets are maximized and each creditor's rightful claims are disposed of as fairly as possible.[57] For example, in terms of MEGs whose businesses are integrated, Irit Mevorach proposes that procedural consolidation would best achieve asset maximization because it would help facilitate the best packaging of the group's assets, which "is especially vital [for] rescues," whether in part or in whole.[58] Collectively, this is beneficial because it helps "preserve the estate (as a whole) and [allows the group] to make an intelligent use of the groups' assets, for the purpose of the continuation of the business."[59]

However, to achieve such procedural coordination in the international context, some of the goals should be to "provid[e] clarity and predictability in the application of the law," treat "similarly situated creditors equally," and ensure fairness such that all creditors and parties "are given a full and fair opportunity to explain their views."[60]

In this realm, there are two different approaches to multijurisdictional coordination: territorialism and universalism.[61]

1. Territorialism

Territorialism, as the name may suggest, prescribes that "the effects of insolvency proceedings should be confined to such property as is located within the territorial jurisdiction of the country in which the proceedings are opened."[62] "Instead of managing [a] company's assets worldwide ... 'state by state' insolvenc[ies]" are conducted.[63] Each court decides, "applying local laws and practices," how to distribute the debtor's assets.[64] In this way, local creditors are protected, and the "unique distinctions between legal regimes" are faced with "minimum interference with domestic policies."[65]

---

57. *See* U.N. COMM'N ON INT'L TRADE LAW, UNCITRAL LEGISLATIVE GUIDE ON INSOLVENCY LAW: PART THREE: TREATMENT OF ENTERPRISE GROUPS IN INSOLVENCY, at 86, U.N. Sales No. E.12.V.16 (2012) [hereinafter UNCITRAL LEGISLATIVE GUIDE PART THREE] (recommending cooperation among foreign jurisdictions in the insolvency of multinational enterprise groups).

58. MEVORACH, INSOLVENCY WITHIN MEGS, *supra* note 48, at 154.

59. *Id.*

60. Samuel L. Bufford, *Coordination of Insolvency Cases for International Enterprise Groups: A Proposal*, 86 AM. BANKR. L. J. 685, 692 (2012).

61. MEVORACH, INSOLVENCY WITHIN MEGS, *supra* note 48, at 65 ("The main dispute regarding how international insolvencies should be dealt with is between two traditional approaches (positioned on the two ends of the 'theoretical spectrum' of this issue)—universalism and territorialism.").

62. *Id.* at 71.

63. *Id.*

64. *Id.*

65. *Id.*

2. Universalism

On the flip side, universalism attempts to put all of the creditors of a given debtor into a unified system for bankruptcy.[66] In its purest and best form, this would mean that the administration of multinational insolvencies would be done by a single court applying a single insolvency law.[67] Instead of splitting the case up into the group members' various jurisdictions, the cases would be put together to be heard in one forum.[68] Further, the court would apply one substantive law to avoid the expense and delay caused by choice-of-law litigation.[69] Of course, to achieve such a result and at the same time prevent forum shopping, it would seem that an international, harmonized substantive law would be required.[70]

C. Meeting Competing Creditors' Expectations

Finally, and most importantly, the way an entity is treated and its assets disposed of, with respect to the group, should aim to match creditors' expectations. In the group context, this is difficult because (1) "under national laws, each entity has separate legal status, with a separate body of shareholders, a separate body of creditors, and (presumably) separate assets"[71] and (2) a "[c]orporate group's structural dynamism makes it difficult to pre-determine third-party expectations about the corporate group's structure."[72] To this point, it seems fair to say that many times the group's creditors have competing expectations. Initially, "it has been stressed that insolvency law should respect rights obtained by creditors prior to insolvency";[73] however, this goal of insolvency has been considered too narrow. Insolvency goals should be widened to incorporate fairness, which "requires taking into account all relevant parties that are affected by the relevant law"[74] and sometimes redistribution.[75]

Related to this point and limited liability above, the central problem in the group enterprise area can be characterized as a problem of reliance.

> On the one hand, "[w]here the business enterprise group is comprised of separate legal entities, the integration of financial systems and the co-

66. Jay Lawrence Westbrook, *A Global Solution to Multinational Default*, 98 MICH. L. REV. 2276, 2277 (2000).

67. *See id.* at 2292 ("There are two elements necessary to a universalist convention for international bankruptcy: a single law and a single forum to govern each multinational case.").

68. MEVORACH, INSOLVENCY WITHIN MEGS, *supra* note 48, at 66.

69. *Id.*

70. Especially if, as some scholars have suggested, universalism seeks to achieve "equal treatment of all creditors on a global basis." *See id.* at 67; *see also* John A. E. Pottow, *The Myth (And Realities) of Forum Shopping in Transnational Insolvency*, 32 BROOK. J. INT'L L. 785, 787–90 (2007) (stating that the predictability that comes with universalism is a necessary prerequisite to forum shopping, but noting that territorialism is still worse in this respect).

71. Bufford, *supra* note 60, at 690.

72. Wouters & Raykin, *supra* note 49, at 397.

73. MEVORACH, INSOLVENCY WITHIN MEGS, *supra* note 48, at 111.

74. *Id.* at 117–18.

75. *Id.* at 113–14.

> mingling of supplies and common control can lead less sophisticated creditors into believing that they are dealing with an entity with a reputation that leads them to believe it is a good credit risk, when, in reality, their legal relationship is with a separate legal personality."[76]

Alternatively, creditors' expectations to look only to an individual entity may be upset by treating the entity separately in insolvency by "fail[ing] to recognize how assets have been transferred between entities during the financially healthy years and disadvantage creditors that have claims against the entity that continually transferred its wealth to the parent."[77] On the other hand, other investors and parent corporations may rely on the separate legal existence of the entity from the group to shield it from intragroup claims, allowing it to innovate and take more risks, striving for more efficient operations.[78] Of course, solely from the creditor's perspective, this seems to indicate that "creditors have selected their debtor with deliberation and have thus acquired the right that the law must respect their decision for this particular debtor."[79] At least to one author, although it has not been examined or tested, this seems to be a "shaky" justification.[80]

Perhaps one of the best ways to meet creditors' expectations in this area and balance their competing goals is to have a system that generates some predictability as to what is considered fair. "Clear rules can reduce causes for litigation as well as enhance expeditious dispute resolution," allow parties in insolvency to "calculate risk and price the transaction with the debtor accordingly," and support fairness.[81]

III. POSSIBLE SOLUTIONS – TRACING WHAT HAS BEEN PROPOSED ON THE INTERNATIONAL LEVEL TO COORDINATE MULTINATIONAL ENTERPRISE GROUP INSOLVENCY AND PROPOSING A NEW APPROACH TO THE EXISTING FRAMEWORK

A. UNCITRAL Progress

Within the insolvency law arena, striving to modernize and harmonize rules of international business, UNCITRAL has already offered some solutions and guidance for moving forward.[82] For example, Working Group V has drafted Model Legislative

---

76. Janis Sarra, *Oversight and Financing of Cross-Border Business Enterprise Group Insolvency Proceedings*, 44 TEX. INT'L L. J. 547, 550 (2009).

77. *Id.* at 551.

78. *See id.* at 550 ("The business enterprise group is a risk reduction strategy in the sense that claims against one entity for particular kinds of conduct in a jurisdiction will attach only to that legal entity, except in very limited circumstances . . . .").

79. *See* Christoph G. Paulus, *Group Insolvencies—Some Thoughts about New Approaches*, 42 TEX. INT'L L. J. 819, 825 (2007) (noting this argument).

80. *Id.*

81. MEVORACH, INSOLVENCY WITHIN MEGS, *supra* note 48, at 270; *see also* Bufford, *supra* note 60, at 693–94 (noting that "[c]larity of rules and predictability in their application is important to minimizing the transaction costs of an insolvency proceeding" and discussing specific benefits of predictability).

82. *About UNCITRAL*, UNCITRAL, http://www.uncitral.org/uncitral/en/about_us.html (last visited May 5, 2015).

Provisions on Cross-Border Insolvency, completed a Legislative Guide on Insolvency Law, and written about, as well as discussed, the treatment of enterprise groups in insolvency.[83]

1. UNCITRAL Model Law on Cross-Border Insolvency

Starting with the genesis and foundation of work in this area, UNCITRAL Model Law on Cross-Border Insolvency, adopted in 1997, sets out to

> provide effective mechanisms for dealing with cases of cross-border insolvency so as to promote the objectives of:
>
> (a) Cooperation between the courts and other competent authorities of this State and foreign States involved in cases of cross-border insolvency;
>
> (b) Greater legal certainty for trade and investment;
>
> (c) Fair and efficient administration of cross-border insolvencies that protects the interests of all creditors and other interested persons, including the debtor;
>
> (d) Protection and maximization of the value of the debtor's assets; and
>
> (e) Facilitation of the rescue of financially troubled businesses, thereby protecting investment and preserving employment.[84]

To achieve these objectives, the UNICTRAL Model Law on Cross-Border Insolvency lays out provisions that strive to ensure "access, recognition, relief (assistance), and cooperation."[85]

Importantly, what is available to a representative depends upon a dual framework that distinguishes between main proceedings and non-main proceedings.[86] A main proceeding is "one taking place where the debtor had its centre of main interests (COMI) at the date of commencement of the foreign proceeding."[87] In theory, the main proceeding should take the lead in managing the insolvency process.[88] Here, COMI is not defined, but it is presumed to be the registered office

---

83. *See Working Group V 2001 to Present: Insolvency Law*, UNCITRAL, http://www.uncitral.org/uncitral/en/commission/working_groups/5Insolvency.html#1995-1999:%20Insolvency%20law (last visited June 15, 2015) (listing documents that include notes, proposals, and working model laws of Working Group V).

84. U.N. COMM'N ON INT'L TRADE LAW, UNCITRAL MODEL LAW ON CROSS-BORDER INSOLVENCY WITH GUIDE TO ENACTMENT AND INTERPRETATION, pmbl., U.N. Sales No. E.14.V.2 (2014) [hereinafter UNICITRAL MODEL LAW WITH GUIDE].

85. Wouters & Raykin, *supra* note at 49, at 391.

86. Bufford, *supra* note 60, at 705–06 (stating that the UNCITRAL Model Law and the European Union Regulation recognize a foreign proceeding as either a main proceeding or a non-main proceeding); UNCITRAL MODEL LAW WITH GUIDE, *supra* note 84, art. 17 (describing foreign main and non-main proceedings, when the proceedings should be recognized, and the effects of such recognition).

87. UNCITRAL MODEL LAW WITH GUIDE, *supra* note 84, para. 31.

88. *Id.*

or habitual residence of the debtor.[89] On the other hand, a non-main proceeding is "one taking place where the debtor has an establishment."[90] Overall, these provisions attempt to balance the playing field by providing equal rights to foreign and local creditors, while at the same time stopping short of subjecting the foreign representative or its assets to the jurisdiction of a foreign court automatically by mere application.[91]

So far, it might be said that UNCITRAL has come a long way on insolvency—a version of the Model Law has been adopted in twenty-two countries, including the United States.[92] However, UNCITRAL has yet to specifically address the treatment of enterprise groups with a model law.[93]

2. UNCITRAL Legislative Guide on Insolvency Law

In lieu of a model law, UNCITRAL's Working Group V has chosen to address the issue of MEG insolvency via legislative guidance. In 2005, UNCITRAL published a Legislative Guide on Insolvency Law, now Parts One and Two.[94] And in 2010, it published Part Three on the treatment of enterprise groups in insolvency.[95] Taken as a whole, the Legislative Guide on the treatment of enterprise groups in insolvency seeks to "permit, in both domestic and cross-border contexts, treatment of the insolvency proceedings of one or more enterprise group members . . . to address the issues particular to insolvency proceedings involving those groups and to achieve a better, more effective result for the enterprise group as a whole and its creditors."[96] To achieve this result, the Legislative Guide applies recommendations proposed in Part Two for the insolvency of group members in a domestic context unless otherwise indicated.[97]

Within Part Two of the general Legislative Guide, section five, subsection C addresses the treatment of corporate groups in insolvency.[98] After the discussion of some of these issues in Legislative Guide Part Two, Part Three takes the treatment of enterprise groups head on. For the most part, though, Working Group V withholds substantive measures for the treatment of enterprise groups to the domestic context and opts for procedural coordination on the multinational stage.[99]

---

89. *Id.*

90. *Id.* para. 32.

91. *Id.* arts. 10, 13 & paras. 26–27 (providing for Article 10, which limits jurisdiction, and Article 13, which ensures same rights for local and foreign creditors, and interpretation of the thrust and application of these articles).

92. *Status: UNCITRAL Model Law on Cross-Border Insolvency (1997)*, UNCITRAL, http://www.uncitral.org/uncitral/en/uncitral_texts/insolvency/1997Model_status.html (last visited June 15, 2015) (listing States that have adopted legislation based on the UNCITRAL Model Law on Cross-Border Insolvency).

93. *See* UNCITRAL LEGISLATIVE GUIDE PART THREE, *supra* note 57, at 1 (noting the model law was limited to individual group members, not enterprise groups).

94. U.N. COMM'N ON INT'L TRADE LAW, LEGISLATIVE GUIDE ON INSOLVENCY LAW, U.N. Sales No. E.05.V.10 (2005) [hereinafter UNCITRAL LEGISLATIVE GUIDE PARTS 1 & 2].

95. UNCITRAL LEGISLATIVE GUIDE PART THREE, *supra* note 57.

96. *Id.* at 1–2.

97. *Id.* at 1.

98. UNCITRAL LEGISLATIVE GUIDE PARTS 1 & 2, *supra* note 94, at 276–79.

99. *Compare* UNCITRAL LEGISLATIVE GUIDE PART 3, *supra* note 57, at 71–74, recommendations 219–231 (laying out guidelines for asset consolidation remedies available to domestic enterprise groups

Still, a discussion of both sets of measures is informative in discussing what may be an appropriate model law in this area.

To start, considering how UNCITRAL defines an enterprise group may be helpful. In UNCITRAL terms, an enterprise group is "two or more enterprises that are interconnected by control or significant ownership."[100] Here, an "enterprise" is "any entity, regardless of its legal form, that is engaged in economic activities and may be governed by the insolvency law,"[101] and "control" exists when one entity has "the capacity to determine, directly or indirectly, the operating and financial policies of an enterprise."[102] Further, within an enterprise group, the use of "parent" refers to "the entity that controls members of an enterprise group and the term 'controlled group member' [] refer[s] to those members controlled by the parent, irrespective of their legal structure."[103]

Using this term, UNCITRAL sets out recommendations on how to treat an enterprise group within the domestic context. For the purposes of this Note, the focus will be on the recommendations concerning the treatment of assets within an enterprise group upon insolvency, rather than the adapted but familiar procedural provisions applied to enterprise groups. The provisions related to the treatment of assets within an enterprise group include provisions dictating when avoidance and substantive consolidation may take place within the group context.[104] The avoidance provisions prompt drafters to specify whether to permit the court to take into account that the transaction took place within the enterprise group and if so, which circumstances will be considered and in what way.[105] The circumstances to be considered, Working Group V mentions, may include: the relationship between the parties, the degree of integration between the group members, the purpose of the transaction, whether the transaction contributed to the operations of the group as a whole, and whether the transaction granted advantages to enterprise group members or other related persons that would not normally be granted between unrelated parties.[106]

In a similar vein, Working Group V suggests that drafters explicitly permit substantive consolidation, but in doing so, it explicitly limits its availability and describes the effects of substantive consolidation.[107] As a preliminary matter, drafters are instructed to mention that "insolvency law should respect the separate legal identity of each enterprise group member," subject only to the limited grounds provided by the law.[108] These grounds are limited to circumstances where: (a) the court finds that "the assets or liabilities of the enterprise group members are

---

when certain conditions are met), *with id.* at 89, 100–03 (recycling Model Law-type measures to coordinate procedurally the insolvency of enterprise group members).

100. *Id.* at 2.

101. *Id.*

102. *Id.*

103. *Id.* at 2–3.

104. *Id.* at 51–52, recommendations 217–218 (listing provisions for avoidable transactions), 71–74, recommendations 219–231 (laying out provisions to govern the availability of substantive consolidation).

105. UNCITRAL LEGISLATIVE GUIDE PART THREE, *supra* note 57, at 51, recommendation 217.

106. *Id.* at 51–52, recommendations 217–218.

107. *See id.* at 71, recommendation 219 (laying out circumstances in which substantive consolidation may be available).

108. *Id.*

intermingled" such that they cannot be parsed without "disproportionate expense or delay,"[109] or (b) the court finds that "the enterprise group members are engaged in a fraudulent scheme or activity with no legitimate business purpose and that substantive consolidation is essential to rectify [it]."[110] Even if substantive consolidation is ordered, though, UNCITRAL recommends that the court allow some assets be excluded in certain enumerated circumstances.[111] The effect of substantive consolidation under this type of regime would be that the assets and liabilities of the substantively consolidated group would be treated as a single estate,[112] claims and debts between these group members would be extinguished,[113] and claims against the substantively consolidated group would be treated as if they were claims against the single insolvency estate.[114] In the domestic context, it is important to note that this type of provision covers some traditional reasons that prompt courts to order substantive consolidation,[115] but it still fails to provide coverage of ways in which the assets of one entity may be transferred to another via other common law causes of action (intragroup claims), which to some group members could be considered as serving a legitimate business purpose (especially for the enterprise group as a whole).

Possibly even more inadequate, these provisions are not recommended in the MEG context, where differences among jurisdictions as to when to disregard the corporate entity and transfer assets from one entity to another, either in whole or in part through judgment or consolidation, may be even more divergent. Instead of taking this approach, UNCITRAL has reached for what some describe as "universalism doubly modified,"[116] opting for procedural coordination instead in the form of watered-down cooperation and communication.[117] As described by one author, "Working Group V has essentially waved the white flag . . . on addressing head-on the problem of enterprise groups, even though it acknowledges that such groups are 'the most common form of business model.'"[118]

To address this problem, some scholars have proposed to adapt these existing models to provide more comprehensive treatment of the MEG in insolvency. Among the models are proposals to have an umbrella proceeding for the insolvency cases of the various enterprise group entities that will be commenced in the enterprise center of main interest (ECOMI) State, where the enterprise's management headquarters or head office is located.[119] Here, for the most part, the

109. *Id.* at 72, recommendation 220(a).

110. *Id.* recommendation 220(b).

111. UNCITRAL LEGISLATIVE GUIDE PART THREE, *supra* note 57, at 72, recommendation 221.

112. *Id.* recommendation 224(a).

113. *Id.* at 73, recommendation 224(b).

114. *Id.* recommendation 224(c).

115. *See supra* notes 26–30 and accompanying text.

116. Mevorach, *Towards a Consensus*, *supra* note 1, at 422 (internal quotation marks omitted).

117. *See* UNCITRAL LEGISLATIVE GUIDE PART THREE, *supra* note 57, at 100–03, recommendations 240–245 (detailing measures for cross-court communication and cooperation); *see also* Mevorach, *Towards a Consensus*, *supra* note 1, at 422 ("[The Working Group's approach] attempts to expand the modified universalism-based concepts available in UNCITRAL Model Law for single companies. However, when applying it to groups the Working Group eventually focused mainly on cooperation.").

118. Sexton, *supra* note 5, at 831 (quoting a draft of Part Three that was published in the final version, UNCITRAL LEGISLATIVE GUIDE PART THREE, *supra* note 57, at 84).

119. Bufford, *supra* note 60, at 691–92; *cf.* RALPH R. MABEY, PROSPECTIVE PRINCIPLES FOR

ECOMI's procedural and substantive insolvency laws would govern, but individual entity COMIs' substantive law for avoiding proceedings, determining the merits of claims, and ranking of claims would still govern.[120]

B. The German Stock Corporation Act of 1965

While UNCITRAL has made laudable efforts forward toward the procedural coordination of groups in insolvency, the question still remains: How can procedural coordination over integrated multinational enterprise groups be achieved without a harmonized or standard way of assessing when an entity is integrated with others, such that it is considered part of a group, where its assets may be wholly or partially consolidated? This Note argues that the answer is it cannot. Ultimately, because of the differences in law among jurisdictions, procedural coordination—more specifically the selection and implementation of a COMI model for multinational groups—is impossible without a model law that outlines when a group will be treated as an enterprise (its corporate form disregarded) and its assets commingled, in whole or in part. Recognizing this necessity, this Note analyzes whether the German Stock Corporation Act of 1965 could be a great starting place for an UNCITRAL model law in this area.

1. The Act

Under the German Stock Corporation Act of 1965, corporate entities may be considered related, or affiliated, enterprises in five different cases:

1. *Contractual Enterprises* – When parties have agreed through an enterprise agreement to be related enterprises.[121]

2. *Majority Interest Ownership* – When one enterprise owns a majority interest, or holds a majority of votes, in another independent enterprise[122]

3. *Controlled or Controlling Enterprises* – When one enterprise exercises, directly or indirectly, a controlling influence over another enterprise[123]

COORDINATION OF MULTINATIONAL CORPORATE GROUP INSOLVENCIES 9–10 (2012), *available at* http://iiiglobal.org/component/jdownloads/finish/362/5953.html (rejecting the notion of center of main interest, but acknowledging advantages to having some "Group Center" out of which the organization is controlled).

120. Bufford, *supra* note 60, at 691–92 (listing provisions of ECOMI model proposal).

121. Aktiengesetz [AktG] [Stock Corporation Act], Sept. 6, 1965, BGBL I at 1089, arts. 291–292, last amended by Restrukturierungsgesetz, Dec. 9, 2010, BGBL I at 1900, art. 6 (Ger.), *translated in* NORTON ROSE FULBRIGHT, STOCK CORPORATION ACT: TRANSLATION AS AT 1 DECEMBER 2011 §§ 291–292 (2011), *available at* http://www.nortonrosefulbright.com/files/german-stock-corporation-act-2010-english-translation-pdf-59656.pdf; *accord* Dieter Schoner, *U.S. Multinational Enterprises Under German Law*, 3 INT'L BUS. LAW. 271, 279 (1975); GERHARD WIRTH ET AL., CORPORATE LAW IN GERMANY 208–09 (2d ed. 2010).

122. AktG art. 16, *translated in* NORTON ROSE FULBRIGHT, *supra* note 121, § 16; *accord* Schoner, *supra* note 121, at 279; WIRTH ET AL., *supra* note 121, at 208.

123. AktG art. 17, *translated in* NORTON ROSE FULBRIGHT, *supra* note 121, § 17; *accord* Schoner, *supra* note 121, at 279; WIRTH ET AL., *supra* note 121, at 208.

4. *Combines (Centralized Management)* – When one or more enterprises, which are controlled, or with the controlling enterprise, are a part of a centralized management structure,[124] and

5. *Mutually Participating Enterprises* – When one enterprise holds one-fourth of another enterprise's shares, or one-fourth of an enterprise's shares are held by another enterprise.[125]

In general, these cases fall into two major categories that provide a dual approach to liability.[126] First, a corporate entity may become a related enterprise as a contractual concern. In terms of contractual enterprises, enterprise agreements may be:

> control [domination] agreement . . . agreements to transfer all profits [and losses] to another enterprise . . . pooling of profit agreements [] by which independent enterprises undertake to pool their profits [wholly or partially], [and] business lease or surrender agreements . . . by which an enterprise leases its entire business to another or otherwise surrenders its operation.[127]

A major benefit that comes with making such a control agreement is that the parent corporation may "exercise far-reaching management powers over the subsidiary and its operations."[128] In fact, the parent can even direct the subsidiary to take actions detrimental to it, provided, however, that the actions meet two conditions: (a) they are in the best interests of the corporate group, and (b) they do not make the subsidiary insolvent.[129] Ultimately, though, this contractual relationship imposes a duty upon the parent corporation "to compensate the subsidiary for all annual deficits incurred by such controlled entity during the contract period."[130] Importantly, this duty is formed regardless of whether there is actually a relationship between the parent and subsidiary and regardless of whether the subsidiary's losses are actually caused by the parent corporation.[131]

Alternatively, the second way a corporate entity may become a related enterprise is as a de facto or factual concern.[132] The factual concern group comes into existence not by a control agreement but by statute[133] once one of four criteria,

---

124. AktG art. 18, *translated in* NORTON ROSE FULBRIGHT, *supra* note 121, § 18; *accord* Schoner, *supra* note 121, at 279; WIRTH ET AL., *supra* note 121, at 208.

125. AktG art. 19, *translated in* NORTON ROSE FULBRIGHT, *supra* note 121, § 19; *accord* Schoner, *supra* note 121, at 279; WIRTH ET AL., *supra* note 121, at 208. Please note that these enterprises must be corporations with a registered office in Germany to be considered a group. AktG art. 19(1), *translated in* NORTON ROSE FULBRIGHT, *supra* note 121, § 19(1) (limiting the article's reach to "[e]nterprises which have a domestic domicile").

126. Rene Reich-Graefe, *Changing Paradigms: The Liability of Corporate Groups in Germany*, 37 CONN. L. REV. 785, 788 (2005).

127. Schoner, *supra* note 121, at 279 (listing when parties may be subject to an enterprise agreement for purposes of the Stock Corporation Act); *see also* WIRTH ET AL., *supra* note 121, at 208–09 (incorporating more detailed information for what constitutes an enterprise agreement).

128. Reich-Graefe, *supra* note 126, at 788–89.

129. *Id.* at 789.

130. *Id.*

131. *Id.*

132. *Id.* at 790.

133. *See id.* (calling the factual concern category "a 'pure-bred' statutory creation").

mentioned above as (2)–(5), has been met: (a) one corporation owns a majority interest in another,[134] (b) one corporation exercises direct or indirect control over another corporation, (c) one or more corporations are operated under a centralized management system in terms of management and control, or (d) for German enterprises, once one enterprise holds, or is held by, a 25% interest in another enterprise.

The potential upside to a corporation being considered a part of an affiliated group as a matter of factual concern, rather than by contract, is that if it is the controlling entity, it does not automatically have to compensate the controlled subsidiary for any of its losses; however, the trade-off is that "the controlling enterprise cannot impose directives which are to the disadvantage of the controlled enterprise without providing adequate compensation."[135] As described by one scholar, what this means is that "in any case of a particular interference by the parent company in the subsidiary's management—which interference is disadvantageous to the independent business interests of the subsidiary—the parent company shall compensate the subsidiary for any and all damages sustained as a result of such singular interference," leaving liability to be analyzed on a case-by-case, interference-by-interference basis.[136]

2. How It Has Been Applied

Unfortunately, throughout its history, the German Stock Corporation Act of 1965 has not been strictly applied. In fact, there has only been "one successful suit against a parent company based on de facto concern compensation liability."[137] To some extent, this has been the result of two factors: (1) the original act only applied to German stock corporations,[138] which as a result left limited liability companies, known in Germany as *GmbHs*, out of its reach,[139] and (2) the complication of

134. "Majority holdings [are] calculated based on the registered share capital or the voting rights." WIRTH ET AL., *supra* note 121, at 208.

135. Schoner, *supra* note 121, at 280.

136. Reich-Graefe, *supra* note 126, at 791.

137. *Id.* at 792.

138. This statement should be qualified with some explanation. The definitions in the Stock Corporations Act describing affiliation, control, and company groups "are not specific to *AGs* [or stock corporations] but apply to all kinds of entities. [However,] the Act directly regulates the consequences of a relationship of control only for situations in which the controlled enterprise is an *AG* or a partnership limited by shares (*KGaA*)." WIRTH ET AL., *supra* note 121, at 207. In the case of a controlled entity that is not *AG* or *KGaA*, such as a *GmbH* or a partnership, "the provisions relevant to the respective legal form" of the controlled entity will govern. *Id.* Nonetheless, there may be supplemental case law that imposes group-like liability or provisions. *See id.* ("[T]here is no codified law governing company groups, but merely rules developed from the case law, some of which have been developed from the provisions governing groups of *AGs*."); *see also infra* notes 141–144 and accompanying text (discussing the German Federal Supreme Court's parallel doctrinal development over *GmbHs* in this area). In contrast, the controlling entity can be anything – a corporation, a partnership, a cooperative, a foundation, a natural person, a non-commercial partnership, and even the German government. WIRTH, ET AL., supra note 121, at 207.

139. Reich-Graefe, *supra* note 126, at 794.

procedurally separating particular instances of interference seemed to prove too much.[140]

Despite the lack of cases based on the statute per se, there is much to be gleaned from German case law in this area in terms of formulating a model law sculpted from the Stock Corporation Act of 1965. Recognizing the holes in the Stock Corporation Act's framework and working to fix some of its initial problems, the German Federal Supreme Court developed a separate, parallel legal doctrine to apply to "qualified de facto concern[s]," encompassing *GmbH* subsidiaries rather than corporations.[141] Initially, this doctrine operated very much like the Corporation Act it paralleled—it came into play when a "parent company was found to be 'permanently and extensively' involved in the management of its subsidiary."[142] However, the doctrine took the remedy a few steps further and made it easier to use—once the interfering relationship between the parent and subsidiary was established, the court gave the plaintiff the benefit of a rebuttable presumption such that if the parent was unable to defend itself, "it was held personally liable to the creditors of the subsidiary for all of the subsidiary's obligations."[143] This has been noted as significant by some scholars because it forced majority shareholders to present exculpatory evidence that their interference with the subsidiary was not detrimental, and it blended the dual liability framework of the factual and contractual concerns in the Stock Corporation Act.[144]

Ultimately, though, beginning in the early 2000s, the momentum toward a comprehensive scheme of intragroup liability for enterprise groups dissipated, and much of the progress was erased.[145] In its *Bremer Vulkan* decision, the German Federal Supreme Court essentially withdrew the "qualified de facto concern" doctrine, opting instead to protect GmbH subsidiaries through the stated capital requirements imposed by the German Limited Liability Company Act.[146] To some, it appeared that the Court was "not willing to continue its path down the rocky road of corporate liability within corporate groups which, in the past, had been guided mainly by considerations focusing on the power architecture within the corporate group."[147] Instead of basing liability on the corporate architecture, the Court opted for a "differentiated system of management's liability, focusing on the financial interests of the corporate daughter and the related protective duties of the management."[148] As alluded to previously, the protection of the controlled entity, and thereby liability to the parent, or controlling entity, was "limited to maintenance of its base capital [requirements] and the safeguard of its existence—both of which imply a duty on the management's side to appropriately consider the daughter's own

140. *Id.* at 791–92.

141. *Id.* at 794–97.

142. *Id.* at 796 (footnote omitted).

143. *Id.*

144. *Id.* at 796–97.

145. *See* Reich-Graefe, *supra* note 126, at 799 (describing a setback following the Supreme Court's *Bremer Vulkan* decision).

146. *Id.* at 800–01.

147. Peer Zumbansen, *Liability Within Corporate Groups (*Bremer Vulkan*) – Federal Court of Justice Attempts the Overhaul*, 3 GERMAN L.J., no. 1, 2002, para. 6, *available at* http://www.germanlawjournal.com /index.php?pageID=11&artID=124.

148. *Id.* para. 7.

interests."[149] To some, this created a simpler approach because it drew a bright line by severing an analysis of relationships to determine liability and looking only to the actors.[150] But it remained to be seen exactly what duties management owed. Ultimately, the decision left some uncertainty, and to an outsider, it could have "look[ed] very distantly like [the] 'business judgment rule.'"[151]

C. *Prospective Alteration of the German Stock Corporation Act of 1965 and Application within the UNCITRAL Framework*

Although not perfect in its raw form, adopting a UNCITRAL model law styled after the German Stock Corporation Act of 1965 may be a great starting place for harmonizing the existing variations in enterprise liability and providing more predictability in the allocation of assets that takes place in many MEG insolvencies.

1. Benefits of Starting with a Model Law Like the Stock Corporation Act

The German Stock Corporation Act of 1965 could be a great starting place for harmonizing the existing variations in enterprise liability in the form of a UNCITRAL model law for four reasons: (1) it takes a prospective approach to determining intragroup liability, potentially eliminating the need for as much post-hoc litigation; (2) it does not limit its application to certain enterprise structures but is broad enough to account for a number of different forms of enterprise "control"; (3) it takes an intermediate approach to enterprise liability that neither ignores the economic realities of enterprise groups nor completely eradicates limited liability; and (4) in some cases, it permits an entity to exercise control over another one as a matter of prudent business operations of the enterprise, rather than attaching negative connotations to practices that currently take place within an existing legal framework that has yet to keep pace with economic realities.

First, the Stock Corporation Act could be a great starting place for harmonizing existing variations in law in the form of a UNCITRAL model law because it eliminates the need for an enormous amount of post-hoc litigation over whether one entity should be substantively consolidated with another, whether one entity should be liable for directing another entity to take actions for the benefit of the group, and whether transfers between the entities are fraudulent. Instead of relying on these sorts of doctrines to be work-arounds to the existing entity liability system and leaving the field in uncertain terms, it takes the issue head-on and provides five broad guidelines on when entities will be considered part of an enterprise and what a controlling entity will be liable for in the case of the controlled entity's insolvency or detriment via the contractual concern model and the de facto concern model. As a surface level matter, using this type of framework could help increase certainty and would better cater to potential creditors' ability to allocate risk.

---

149. *Id.* para. 8.

150. *See, e.g., id.* para. 12 ("The approach remains [] a straight forward one, exchanging one polar view with another, without allowing for another, possibly more sensitive assessment of the relationships within corporate groups.").

151. *Id.*

For example, in the Nortel Networks litigation presented at the beginning of this Note,[152] using proposals for procedural universalism and a German-esque framework for narrow substantive universalism regarding MEG liabilities, creditors of the U.S. Nortel subsidiary would have been able to predict in advance that some of the assets of the U.S. subsidiary could be pulled from the subsidiary's operations to compensate foreign sister subsidiaries' creditors for prior operating asset transfers and intragroup agreements. Further, beyond creditors being armed with knowledge of this risk in order to price their transactions with Nortel accordingly, using this framework, the court would have been equipped with more knowledge on how to measure and evaluate the claims by not having to try to apply multiple foreign laws, interpreted solely by the advocates.

Second, the Stock Corporation Act could be a great starting place for drafting a UNCITRAL model law with respect to when the corporate form will be disregarded because its definition of "enterprise" is broad enough to encompass the various forms of structural enterprises.[153] By defining affiliation among enterprises in multiple ways: by contract, ownership, and control, the Act avoids having a problem where decentralized management structures escape coverage.

As noted toward the beginning of this Note,[154] one of the major problems drafters have faced in attempting to deal with the MEG problem is that there are innumerable ways corporate groups can organize multinationally in order to serve their profit-maximizing functions,[155] and as regulations, laws, and the economy change, so too does the organization of the corporate group to adapt to them. Given this, any attempt to mold the group must change too. To date, much of the law geared toward ignoring the corporate form has centered on control exercised in traditional management models,[156] but this focus misses the target by skimming over the realities of business conduct. Many organizations operate in a decentralized fashion, and an entity may have control over its operations but still be operating in a way that is aimed at enhancing the wealth of the enterprise group as a whole.

Here, the German Stock Corporation Act remedies some of these problems by adopting a number of ways that an entity can be a part of an enterprise group: contract, ownership, direct or indirect control, centralized management, or mutually participating activities.[157] As a brief example, this type of definition would cover a foreign subsidiary that pursues its own organizational objectives and sends profits to the parent or sister subsidiary as a matter of weekly operations, but does not get direct instructions from the parent under centralized management. Under a basic contract theory or common law control doctrine, it may be unclear whether such a subsidiary is included within the definition of an enterprise group, and as a result, whether group assets could be subject to claims of the subsidiary. However, using the broad definition in the Stock Corporation Act, it is clear that it could.

---

152. *See supra* notes 33–43 and accompanying text.

153. *See supra* note 101 and accompanying text.

154. *See supra* note 8 and accompanying text.

155. *Cf.* Wouters & Raykind, *supra* note 49, at 397–98 (noting the vast array of possible parent-subsidiary relationships and the differences between and among them).

156. *See supra* notes 1–5 and accompanying text.

157. *See supra* notes 128–132 and accompanying text.

Third, the Stock Corporation Act could be a great starting place for a model law recognizing enterprise group liability because it takes an intermediate approach to group liability. Within the framework of the Act, limited liability is not completely eradicated but kept intact unless certain criteria are met, and then, it is only eliminated with respect to the particular transactions that meet the criteria, notwithstanding the contractual concern. This is in line with the insolvency goals discussed at the outset because it recognizes the economic realities within the integrated enterprise groups but prevents complete or partial consolidation of group assets, unless an entity voluntarily assumes liability for or completely detriments the separate entity, respectively. In this sense, by knowing the law in advance, entities and shareholders can plan on which option of liability they would prefer. But either way, the liability burden comes with a benefit, which leads to the next point.

Fourth and finally, the Stock Corporation Act may be a great statute to look to in terms of a model law because in some respects, it reframes the way existing approaches attempt to disregard the corporate form. Rather than relying on premises of fraud or theories of deception to hold enterprise members liable,[158] the Act takes economic realities head-on. It couches liability of an enterprise member not in fraud, but in terms of permissive control and direction of the controlled entity, which may be detrimental to that entity, but beneficial for the enterprise group. In some sense, this may be a more positive way at looking at what strategic managers seek to accomplish and could be an angle to exploit in advancing the cause of intragroup enterprise liability. Instead of just threatening with a stick, the Act gives a carrot to the parent, with the knowledge that if the carrot is abused to the detriment of the controlled entity, there will be a stick.

However, on some level, there will always be a place for fraud. One cannot help but think that some of the claims in insolvency that assert these fraudulent-type causes of action are brought merely because the realities of the economic enterprise and its corresponding legal consequences are seen too late, and at that point, there is not much a claimant can do. From this perspective, this is a lose-lose solution for the parties who each relied on a representation of either debt-fulfillment or a debt-shield.

On some level, the Stock Corporation Act approach seems to alleviate this situation and balance out some of the competing political arguments and complaints regarding liability. On the one hand, it lets parties know in advance what they can rely on in terms of assets. On the other hand, it addresses the stigma attached by some commentators who complain that MEGs exploit the gaps of current legal regimes, especially the separate corporate personality, to their sole advantage.[159] Describing the use of separate entities or intragroup transactions within an enterprise group as exploitation may be too harsh in some circumstances, especially when from a business perspective, the use of separate and disaggregated entities may be most

158. *Cf., e.g.*, UNCITRAL LEGISLATIVE GUIDE PART THREE, *supra* note 57, at 72, recommendation 220(b) ("[T]he court may order substantive consolidation with respect to two or more enterprise group members . . . [w]here the court is satisfied that the enterprise group members are engaged in a fraudulent scheme or activity with no legitimate business purpose and that substantive consolidation is essential to rectify that scheme or activity.").

159. *See, e.g.*, BLUMBERG, MULTINATIONAL CHALLENGE, *supra* note 4, at 59–60 (critiquing modern enterprise law).

sensible in terms of efficiently allocating assets and strategically managing an enterprise for the benefit of shareholders and customers.

2. Limitations of the Stock Corporation Act—Remembering That It Is Just a "Starting Place" and There Is Room for Modification

Despite all of the potential benefits of using the Stock Corporation Act as a model for a UNCITRAL model law, the German Stock Corporation Act should only be a starting place and should be modified in at least a few respects. First and foremost, as the German Federal Supreme Court discovered shortly after the enactment of the Act, any model law modeled after the Stock Corporation Act should cover more entities within its definition of a controlled enterprise than the stock corporation, for example, limited liability companies. Rather than limiting a controlled enterprise to a corporation, all entities should be covered. Here, using UNCITRAL's existing definitions of an entity and an enterprise seems most appropriate because it is broad enough to cover the innumerable types of business entities throughout the globe by covering all "entit[ies], regardless of [their] legal form, that [are] engaged in economic activities and may be governed by the insolvency law."[160]

Next, again deriving from the German case law in this area, the Stock Corporation Act should be modified in its terms to provide for a rebuttable presumption of control once the conditions outlining what constitutes an affiliated relationship have been met. As is pointed out in the case law, it can be very difficult to parse out a parent's interferences with the controlled entity. Many times the controlling entity will have more information regarding its control or activities than outsiders. At the same time, however, all of the ways in which this presumption may be used must be closely monitored in order to prevent complete consolidation and parent liability except for in the most extreme cases.

Along these lines, the German Stock Corporation Act of 1965 may need further modification as to what triggers the parent or sister subsidiary's liability. To form a national consensus, the threshold for ownership in the case of a de facto concern may need to be raised above a majority to trigger liability, or a dimension may need to be added to the contractual approach in order to blunt some of the heavy liability that is incurred by the signing of all-too-familiar intragroup contracts. Alternatively, the grounds for liability under the de facto approach may be further limited or enumerated beyond the simple definition of a detrimental interference. Here, one of the nice things about the German Stock Corporation Act is that presumably a controlling entity can choose what type of liability it will incur. In some cases, it may be more beneficial to keep a controlled entity's books at zero than it would be to pay for and litigate each and every asserted interference.

CONCLUSION

Ultimately, UNCITRAL has come a long way in providing an international legal regime for coordinating insolvency proceedings within different jurisdictions. Even domestically, it has offered more legislative guidance on how to treat enterprise

160. UNCITRAL LEGISLATIVE GUIDE PART THREE, *supra* note 57, at 2.

groups. However, there is still a long way to go. Moving from jurisdictional cooperation with the insolvency of MEGs, hopefully one day there will be at least a procedural mechanism that brings the insolvency of group members all together, recognizing one another. However, if this type of procedural mechanism is to be modeled after the UNCITRAL Model Law, creditors need to be able to determine what the COMI is for a group. To determine this, guidance generally looks to the principal place of business or control. In the group context, from a creditor's perspective, this solution still lacks ultimate success because it is unpredictable as to what liability may attach to the parent via different intragroup claims from foreign jurisdictions. Further, even if enterprise liability would be limited to the extent permitted by the group COMI's substantive laws, this may still be undesirable because of the forum shopping incentive it would create. As a result, in order to achieve maximum universalism in insolvency proceedings, a more harmonized model law as to enterprise liability is required. In step with the insolvency goals articulated in this area, one way to create such harmonization might stem from a UNCITRAL model law derived from the German Stock Corporation Act of 1965, modified in several respects.


T
I
L
J