Texas Law Review

SYMPOSIUM:
TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW
APPLICABLE TO CYBER OPERATIONS

William Banks
Robert E. Barnsby
Rebecca Ingber
Eric Talbot Jensen
Jens David Ohlin
Dinah PoKempner
Shane R. Reeves
Christian Schaller
Michael N. Schmitt
Liis Vihul
Sean Watts

JUNE 2017 VOL. 95 NO. 7 PAGES 1487 TO 1670

Texas Law Review (ISSN 0040-4411) is published seven times a year—November, December, February, March, April, May, and June. The annual subscription price is $47.00 except as follows: Texas residents pay $50.88, and foreign subscribers pay $55.00. All publication rights are owned by the Texas Law Review Association. *Texas Law Review* is published under license by The University of Texas at Austin School of Law, P.O. Box 8670, Austin, Texas 78713. Periodicals Postage Paid at Austin, Texas, and at additional mailing offices.

POSTMASTER: Send address changes to The University of Texas at Austin School of Law, P.O. Box 8670, Austin, Texas 78713.

Complete sets and single issues are available from WILLIAM S. HEIN & CO., INC., 1285 MAIN ST., BUFFALO, NY 14209-1987. Phone: (800) 828-7571.

Single issues in the current volume may be purchased from the *Texas Law Review* Publications Office for $15.00 per copy shipping included. Texas residents, please add applicable sales tax.

The *Texas Law Review* is pleased to consider unsolicited manuscripts for publication but regrets that it cannot return them. Please submit a single-spaced manuscript, printed one side only, with footnotes rather than endnotes. Citations should conform with *The Greenbook: Texas Rules of Form* (13th ed. 2015) and *The Bluebook: A Uniform System of Citation* (20th ed. 2015). Except when content suggests otherwise, the *Texas Law Review* follows the guidelines set forth in the *Texas Law Review Manual on Usage & Style* (13th ed. 2015), *The Chicago Manual of Style* (16th ed. 2010), and Bryan A. Garner, *Black's Law Dictionary* (10th ed. 2014).

Editorial Offices: *Texas Law Review*
727 East Dean Keeton Street, Austin, Texas 78705
(512) 232-1280 Fax (512) 471-3282
admin@texaslrev.com
http://www.texaslrev.com

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 Administration and Strategic Planning, Lecturer.*
ROBERT M. CHESNEY, B.S., J.D.; *Associate Dean for Academic Affairs, Charles I. Francis Professor in Law.*
WILLIAM E. FORBATH, A.B., B.A., Ph.D., J.D.; *Associate Dean for Research, Lloyd M. Bentsen Chair in Law.*
EDEN E. HARRINGTON, B.A., J.D.; *Associate Dean for Experiential Education, Director of William Wayne Justice Center for Public Interest Law, Clinical Professor.*
ELIZABETH T. BANGS, A.B., J.D.; *Assistant Dean for Student Affairs.*
LAUREN FIELDER, B.A., J.D., LL.M.; *Assistant Dean for Graduate and International Programs, Senior Lecturer.*
MICHAEL G. HARVEY, B.A., B.S.; *Assistant Dean for Technology.*
REBECCA E. MELTON, B.A., J.D.; *Assistant Dean for Alumni Relations and 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.*
FRANK B. CROSS, B.A., J.D.; *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. LEON LEBOWITZ, A.B., J.D., LL.M.; *Joseph C. Hutcheson Professor Emeritus.*
BASIL S. 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.S., J.D., M.A.; *Charles I. Francis Professor Emeritus in Law.*

PROFESSORS

JEFFREY B. ABRAMSON, B.A., J.D., Ph.D.; *Professor of Government and Law.*
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.*
MARILYN ARMOUR, B.A., M.S.W., Ph.D.; *Associate Professor of Social Work.*
MARK L. ASCHER, B.A., M.A., J.D., LL.M.; *Hayden W. Head Regents Chair for Faculty Excellence.*
RONEN AVRAHAM, M.B.A., LL.B., LL.M., S.J.D.; *Thomas Shelton Maxey Professor in Law.*
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.*
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, Co-Director of Bernard and Audre Rapoport Center for Human Rights and Justice.*
J. BUDZISZEWSKI, B.A., M.A., Ph.D.; *Professor of Government.*
NORMA V. CANTU, B.A., J.D.; *Professor of Education and Law.*
MICHAEL J. CHURGIN, A.B., J.D.; *Raybourne Thompson Centennial Professor.*
JANE M. COHEN, B.A., J.D.; *Edward Clark Centennial Professor.*
WILLIAM H. CUNNINGHAM, B.A., M.B.A., Ph.D.; *Professor of Marketing Administration.*
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 Philosophy and Law.*
MECHELE DICKERSON, B.A., J.D.; *Arthur L. Moller Chair in Bankruptcy Law and Practice, University Distinguished Teaching Professor.*
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.*
DAVID J. EATON, B.A., M.Sc., M.A., PhD.; *Professor of Public Affairs.*
ZACHARY S. ELKINS, B.A., M.A., Ph.D.; *Associate Professor of Government.*
KAREN L. ENGLE, B.A., J.D.; *Minerva House Drysdale Regents Chair in Law, Founder and Co-Director of Bernard and Audre Rapoport Center for Human Rights and Justice.*
KENNETH FLAMM, A.B., Ph.D.; *Professor of Public Affairs.*
JOSEPH R. FISHKIN, B.A., M.Phil., D.Phil., J.D.; *Professor of Law.*
CARY C. FRANKLIN, B.A., M.S.T., D.Phil., J.D.; *Professor of Law.*
MIRA GANOR, B.A., M.B.A., LL.B., LL.M., J.S.D.; *Professor of Law.*
CHARLES E. GHOLZ, B.S., B.S., Ph.D.; *Associate Professor of Public Affairs.*
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. W. Walker Centennial Chair in Law.*
BENJAMIN G. GREGG, B.A., M.S., Ph.D.; *Associate Professor of Government.*
CHARLES G. GROAT, B.A., M.S., Ph.D.; *Professor of Public Affairs.*
PATRICIA I. HANSEN, A.B., M.P.A., J.D.; *J. Waddy Bullion Professor.*
HENRY T. C. HU, B.S., M.A., J.D.; *Allan Shivers Chair in the Law of Banking and Finance.*

BOBBY R. INMAN, B.A.; *Professor of Public Affairs.*
GARY J. JACOBSOHN, B.A., M.A., Ph.D.; *Professor of Government and Law.*
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.; *John T. Kipp Chair in Corporate and Business Law.*
SUSAN R. KLEIN, B.A., J.D.; *Alice McKean Young Regents Chair in Law.*
ALAN J. KUPERMAN, B.A., M.A., Ph.D.; *Associate Professor of Public Affairs.*
JENNIFER E. LAURIN, B.A., J.D.; *Professor of Law.*
SANFORD V. LEVINSON, A.B., Ph.D., J.D.; *W. St. John Garwood and W. St. John Garwood, Jr. Centennial Chair in Law, Professor of Government.*
ANGELA K. LITTWIN, B.A., J.D.; *Professor of Law.*
VIJAY MAHAJAN, M.S.Ch.E., Ph.D.; *Professor of Marketing Administration.*
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.; *Professor of Architecture.*
SUSAN C. MORSE, A.B., J.D.; *Professor.*
LINDA S. MULLENIX, B.A., M.Phil., J.D., Ph.D.; *Morris and Rita Atlas Chair in Advocacy.*
STEVEN P. NICHOLS, B.S.M.E., M.S.M.E., J.D., Ph.D.; *Professor of Engineering.*
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 Government and Law.*
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.; *Joseph D. Jamail Centennial Chair in Law, University Distinguished Teaching Professor.*
DAVID M. RABBAN, B.A., J.D.; *Dahr Jamail, Randall Hage Jamail and Robert Lee Jamail Regents Chair, University Distinguished Teaching Professor.*
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.; *William Powers, Jr. and Kim L. Heilbrun 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 of Sociology.*
WILLIAM M. SAGE, A.B., M.D., J.D.; *James R. Dougherty Chair for Faculty Excellence.*
LAWRENCE SAGER, B.A., LL.B.; *Alice Jane Drysdale Sheffield Regents Chair.* JOHN
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. McDonald 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.*
TARA A. SMITH, B.A., PH.D.; *Professor.*
DAVID B. SPENCE, B.A., J.D., M.A., Ph.D.; *Professor of Business, Government and Society, and Law.*
JAMES C. SPINDLER, B.A., M.A., J.D., Ph.D.; *The Sylvan Lang Professor of Law, Professor of Business.*
JORDAN M. STEIKER, B.A., J.D.; *Judge Robert M. Parker Endowed Chair in Law, Director of Capital Punishment Center.*
MICHAEL F. STURLEY, B.A., J.D.; *Fannie Coplin Regents Chair.*
JEREMY SURI, A.B., M.A., Ph.D.; *Professor of Public Affairs.*
JEFFREY K. TULIS, B.A., M.A., Ph.D.; *Associate Professor of Government.*
GREGORY J. VINCENT, B.A., J.D., Ed.D.; *Professor, Vice President for Diversity and Community Engagement.*
SRIRAM VISHWANATH, B.S., M.S., Ph.D.; *Associate Professor of Electrical and Computer Engineering.*
STEPHEN I. VLADECK, B.A., J.D., *Professor.*
WENDY E. WAGNER, B.A., M.E.S., J.D.; *Joe A. Worsham Centennial Professor.*
MELISSA F. WASSERMAN, B.S., Ph.D., J.D.; *Professor.*
LOUISE WEINBERG, A.B., LL.M, J.D.; *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., J.D., Ph.D.; *Bernard J. Ward Centennial Professor in Law.*
SEAN H. WILLIAMS, B.A., J.D.; *Professor of Law.*
ZIPPORAH B. WISEMAN, B.A., M.A., LL.B.; *Thos. H. Law Centennial Professor.*
PATRICK WOOLLEY, A.B., J.D.; *Beck, Redden & Secrest Professor in Law.*

ASSISTANT PROFESSORS

JAMES W. MCCLELLAND, B.S., Ph.D.

TIMOTHY D. WERNER, B.A., M.A., Ph.D.

SENIOR LECTURERS, WRITING LECTURERS, AND CLINICAL PROFESSORS

ALEXANDRA W. ALBRIGHT, B.A., J.D.; *Senior Lecturer.*
WILLIAM H. BEARDALL, JR., B.A., J.D.; *Clinical Professor, Director of Transnational Worker Rights Clinic.*
NATALIA V. BLINKOVA, B.A., M.A., J.D.; *Lecturer.*
PHILIP C. BOBBITT, A.B., J.D., Ph.D.; *Distinguished Senior Lecturer.*
HUGH L. BRADY, B.A., J.D.; *Clinical 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 Associate Professor.*
MARY R. CROUTER, A.B., J.D.; *Clinical Professor, 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.*

LISA R. ESKOW, A.B., J.D.; *Lecturer.*
LYNDA E. FROST, B.A., M.Ed., J.D., Ph.D.; *Clinical Associate Professor.*
DENISE L. GILMAN, B.A., J.D.; *Clinical Professor, Director of Immigration Clinic.*
KELLY L. HARAGAN, B.A., J.D.; *Clinical Professor, Director of Environmental Law Clinic.*
HARRISON KELLER, B.A., M.A., Ph.D.; *Senior Lecturer, Vice Provost for Higher Education Policy [at the University of Texas at Austin].*
ANDREW KULL, B.A., B.A., M.A., J.D.; *Distinguished 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.*
JIM MARCUS, B.A., J.D.; *Clinical Professor, Co-Director of Capital Punishment Clinic.*
FRANCES L. MARTINEZ, B.A., J.D.; *Clinical Professor.*
TRACY W. MCCORMACK, B.A., J.D.; *Senior Lecturer, Director of Advocacy Programs.*
F. SCOTT MCCOWN, B.S., J.D.; *Clinical Professor, Director of Children's Rights Clinic.*
RANJANA NATARAJAN, B.A., J.D.; *Clinical Professor, Director of Civil Rights Clinic.*
SEAN J. PETRIE, B.A., J.D.; *Lecturer.*
ELIZA T. PLATTS-MILLS, B.A., J.D.; *Clinical Professor.*
RACHAEL RAWLINS, B.A., M.R.P., J.D.; *Senior Lecturer.*
CHRIS ROBERTS, B.S., J.D.; *Clinical Professor, Director of Criminal Defense Clinic.*
AMANDA M. SCHAEFFER, B.A., J.D.; *Lecturer.*
WAYNE SCHIESS, B.A., J.D.; *Senior Lecturer, Director of The David J. Beck Center for Legal Research, Writing and Appellate Advocacy.*
RAOUL D. SCHONEMANN, B.A., J.D. LL.M.; *Clinical Professor.*
PAMELA J. SIGMAN, B.A., J.D.; *Clinical Professor, Director of Juvenile Justice Clinic.*
DAVID S. SOKOLOW, B.A., M.A., J.D., M.B.A.; *Distinguished Senior Lecturer.*
ELISSA C. STEGLICH, B.A., J.D.; *Clinical Professor.*
STEPHEN SLICK, B.A., M.P.P., J.D.; *Clinical Professor, The Robert S. Strauss Center and The Clements Center for National Security.*
LESLIE L. STRAUCH, B.A., J.D.; *Clinical Professor.*
MELINDA E. TAYLOR, B.A., J.D.; *Senior Lecturer, Executive Director of Kay Bailey Hutchison Center for Energy, Law and Business.*
HEATHER K. WAY, B.A., B.J., J.D.; *Clinical Professor, Director of Entrepreneurship and Community Development Clinic.*
LUCILLE D. WOOD, B.A., J.D.; *Clinical Professor.*

ADJUNCT PROFESSORS AND OTHER LECTURERS

ROBERT J. ADAMS JR., B.S., M.B.A., PH.D.
JAMES B. ADKINS JR., B.A., J.D.
ELIZABETH AEBERSOLD, B.A., M.S.
RICKY ALBERS, B.B.A., M.B.A., J.D.
WILLIAM R. ALLENSWORTH, B.A., J.D.
OWEN L. ANDERSON, B.A., J.D.
ANDREW W. AUSTIN, B.A., M.Phil., J.D.
SAMY AYOUB, B.A., M.Sc. Ph.D.
JACK BALAGIA, B.A., J.D.
CRAIG D. BALL, B.A., J.D.
SHARON C. BAXTER, B.S., J.D.
JERRY A. BELL, B.A., J.D.
MICHAEL L. BENEDICT
ALLISON H. BENESCH, B.A., M.S.W., J.D.
CRAIG R. BENNETT, B.S., J.D.
NADIA BETTAC, B.A., J.D.
MURFF F. BLEDSOE, B.A., J.D.
SUSAN L. BLOUNT, B.A., J.D.
ANNA C. BOCCHINI, B.A., J.D.
DIANA K. BORDEN, 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, B.S., LL.B., J.D.
TOMMY L. BROYLES, B.A., J.D.
PAUL J. BURKA, B.A., LL.B.
ERIN G. BUSBY, B.A., J.D.
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.
REED CLAY JR., B.A., J.D.
ELIZABETH COHEN, B.A., M.S.W., J.D.
KEVIN D. COLLINS, B.A., J.D.
JULIO C. COLON, A.A., B.A., J.D.
JOSEPH E. COSGROVE JR.
STEPHEN E. COURTER, B.S., M.S.B.A.
KASIA SOLON CRISTOBAL, B.A., M.S., J.D.
KEITH B. DAVIS, B.S., J.D.
SCOTT D. DEATHERAGE, B.A., J.D.
DICK DEGUERIN, B.A., LL.B.
MELONIE M. DEROSE, B.A., J.D.
RICHARD D. DEUTSCH, B.A., B.A., J.D.
REBECCA H. DIFFEN, B.A., J.D.
PHILIP DURST, B.A., M.A., J.D.
ELANA S. EINHORN, B.A., J.D.
RACHEL A. EKERY, A.B., J.D.
LUKE J. ELLIS, B.A., J.D.
JAY D. ELLWANGER, B.A., J.D.
RANDALL H. ERBEN, B.A., J.D.
EDWARD Z. FAIR, B.A., M.S.W., J.D.
KAY FIRTH-BUTTERFIELD, B.A., M.B.A., LL.M.
ROSS FISCHER, B.A., J.D.
ANDREW R, FLORANCE
JAMES G. FOWLER, B.A., M.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.
JENNIFER S. FREEL, B.J., J.D.
FRED J. FUCHS, B.A., J.D.
HELEN A. GAEBLER, B.A., J.D.
MICHELLE M. GALAVIZ, B.A., J.D.
RYAN M. GARCIA, B.G.S., J.D.
BRYAN A. GARNER, B.A., J.D.
MICHAEL S. GOLDBERG, B.A., 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.
CLINT A. HARBOUR, B.A., B.A., J.D., LL.M.

ROBERT L. HARGETT, B.B.A., J.D.
MARY L. HARRELL, B.S., J.D.
WILLIAM M. HART, B.A., J.D.
KEVIN V. HAYNES, B.A., J.D.
JOHN R. HAYS, JR., B.A., J.D.
ELIZABETH E. HILKIN, B.A., M.S., J.D.
BARBARA HINES, B.A., J.D.
KENNETH E. HOUP, JR., B.A., J.D.
RANDY R. HOWRY, B.J., J.D.
BART W. HUFFMAN, B.S.E., J.D.
MONTY G. HUMBLE, B.A., J.D.
JENNIFER D. JASPER, B.S., M.A., J.D.
WALLACE B. JEFFERSON, B.A., J.D.
CHRISTOPHER S. JOHNS, B.A., L.L.M., J.D.
AARON M. JOHNSON, B.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, B.A., M.Ed., Ph.D.
SCOTT A. KELLER, B.A., J.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.
MICHAEL R. KRAWZSENEK, B.S., J.D.
LARRY LAUDAN, B.A., M.A., Ph.D.
JODI R. LAZAR, B.A., J.D.
KEVIN L. LEAHY, B.A., J.D.
CYNTHIA C. LEE, B.S., B.A., M.A., J.D.
DAVID P. LEIN, B.A., M.P.A., J.D.
KEVIN LEISKE
ANDRES J. LINETZKY, B.A., LL.M.
JAMES LLOYD LOFTIS, B.B.A., J.D.
ANDREW F. MACRAE, B.J., J.D.
MARK F. MAI, B.B.A., J.D.
ANDREA M. MARSH, B.A., J.D.
HARRY S. MARTIN, A.B., M.L.S., J.D.
LAUREN S. MARTIN, B.S., J.D.
ERIN D. MARTINSON, B.A., J.D.
MIMI MARZIANI, B.A., J.D.
LORI R. MASON, B.A., J.D.
PETER C. MCCABE, 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.
EDWIN G. MORRIS, B.S., J.D.
JAMES C. MORRISS III, B.S., J.D.
SARAH J. MUNSON, B.A., J.D.
GEORGE D. MURPHY JR., B.B.A., J.D.
JOHN A. NEAL, B.A., J.D.
CLARK M. NEILY,, B.A. J.D.
JUSTIN A. NELSON, B.A., J.D.
MANUEL H. NEWBURGER, B.A., J.D.
MARTHA G. NEWTON, B.A., J.D.
HOWARD D. NIRKEN, B.A., M.P.Aff, J.D.
CHRISTINE S. NISHIMURA, B.A., J.D.
DAVID G. NIX, B.S.E., LL.M., J.D.
JOSEPH W. NOEL, B.S.E., J.D., M.S.L.S.
JANE A. O'CONNELL, B.A., M.S., J.D.
PATRICK L. O'DANIEL, B.B.A., J.D.
LISA M. PALIN, B.A., M.Ed., M.F.A., J.D.
MARK L. PERLMUTTER, B.S., J.D.
EDSON PETERS, LL.B., LL.M., PH.D.
JONATHAN PRATTER, B.A., M.S.L.I.S., J.D.
MARGARET K. REIN, B.A., J.D.
DAWN REVELEY, 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.
BETTY E. RODRIGUEZ, B.S.W., J.D.
MICHELLE L. ROSENBLATT, B.A., J.D.
JAMES D. ROWE, B.A., J.D.
MATTHEW C. RYAN, B.A., J.D.
MARK A. SANTOS, B.A., J.D.
MICHAEL J. SCHLESS, B.A., J.D.
SUSAN SCHULTZ, B.S., J.D.
AMY J. SCHUMACHER, B.A., J.D.
SUZANNE SCHWARTZ, B.J., J.D.
RICHARD J. SEGURA, JR., B.A., J.D.
STACEY ROGERS SHARP, B.S., J.D.
DAVID A. SHEPPARD, B.A., J.D.
HON. ERIC M. SHEPPERD, B.A., J.D.
TRAVIS J. SIEBENEICHER, B.B.A, J.D.
RONALD J. SIEVERT, B.A., J.D.
AMBROSIO A. SILVA, B.S., J.D.
STUART R. SINGER, A.B., J.D.
STEPHEN T. SMITH, B.A., M.S.
BARRY T. SMITHERMAN, B.B.A., M.P.A., J.D.
LYDIA N. SOLIZ, B.B.A., J.D.
JAMES M. SPELLINGS, JR., B.S., J.D.
MATTHEW R. STEINKE, B.A., M.L.I.S., J.D.
WILLIAM F. STUTTS, B.A., J.D.
MATTHEW J. SULLIVAN, B.S., J.D.
JEREMY S. SYLESTINE, B.A., J.D.
KEITH P. SYSKA, B.S., J.D.
BRADLEY P. TEMPLE, B.A., J.D.
ROSE THEOFANIS, B.A., J.D.
SHERINE E. THOMAS, B.A., J.D.
CARLY M. TOEPKE, B.A., J.D.
MICHAEL J. TOMSU, B.A., M.B.A., J.D.
TERRY O. TOTTENHAM, B.S., LL.M., J.D.
CARLOS R. TREVINO, M.B.A., LL.M., J.D.
TIMOTHY J. TYLER, B.A., J.D.
SUSAN S. VANCE, B.B.A., J.D.
LANA K. VARNEY, B.A., J.D.
ELEANOR K. VERNON, B.A., J.D.
KEEGAN D. WARREN-CLEM, B.A., J.D., LL.M.
CHRISTOPHER M. WEIMER, B.A., J.D.
WARE V. WENDELL, A.B., J.D.
RODERICK E. WETSEL, B.A., J.D.
BENJAMIN B. WHITTENBURG, B.B.A., M.P.A., J.D.
RANDALL B. WILHITE, B.B.A., J.D.
DAVID G. WILLE, B.S.E.E., M.S.E.E., J.D.
ANDREW M. WILLIAMS, B.A., J.D.
JAMES C. WINTERS, B.A., J.D.
TRAVIS M. WOHLERS, B.S., PH.D., J.D.
STEPHEN M. WOLFSON, B.A., M.S., J.D.
DENNEY L. WRIGHT, B.B.A., J.D., LL.M.
DANIEL J. YOUNG, B.A., J.D.
EVAN A. YOUNG, A.B., B.A., J.D.
ELIZABETH M. YOUNGDALE, B.A., M.L.I.S., J.D.

VISITING PROFESSORS

SAMUEL L. BRAY; *Harrington Faculty Fellow.*
BENNETT CAPERS, B.A., J.D.
VICTOR FERRERES, J.D., LL.M., J.S.D.
GRAHAM B. STRONG, B.A., J.D., LL.M.
ANDREW K. WOODS, A.B., J.D., Ph.D.

* * *

Texas Law Review

Volume 95 2016–2017

* * *

Texas Law Review

Volume 95, Number 7, June 2017

SYMPOSIUM:
TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW
APPLICABLE TO CYBER OPERATIONS

* * *

State Responsibility and Attribution of Cyber Intrusions After *Tallinn 2.0*

William Banks*

On July 22, 2016, WikiLeaks released a collection of more than 18,000 e-mails from the formally impartial Democratic National Committee (DNC) that showed bias against the Bernie Sanders campaign and a cozy relationship between the DNC and its top officials with the Hillary Clinton campaign.[1] Apparently timed to embarrass and disrupt the DNC and the Clinton campaign on the eve of the Democratic National Convention, the leak led to the resignation of key DNC officials, a formal apology to Senator Sanders and his supporters, and lingering impressions that the DNC was anything but neutral during the campaign and that the Clinton campaign could not be trusted.[2] On October 7, WikiLeaks began serial publication of thousands of e-mails to and from John D. Podesta, Mrs. Clinton's campaign manager. Released nearly daily over the last month of the campaign, the Podesta e-mails led to news reports and manipulation on social media that focused on tensions inside the Clinton campaign and campaign insiders' opinions that Clinton was not a strong candidate, among other things.[3] A second batch of DNC e-mails was released on November 6, two days before the election.[4]

The Federal Bureau of Investigation (FBI) first contacted the DNC in September 2015 to warn the Democrats that at least one of their computer systems had been compromised by hackers linked to the Russian

---

* Board of Advisors Distinguished Professor, Syracuse University College of Law; Professor of Public Administration and International Affairs, Maxwell School of Citizenship and Public Affairs, Syracuse University. The author thanks Taylor Henry, Syracuse University College of Law, J.D. 2018, for excellent research assistance.

1. Eric Lipton et al., *The Perfect Weapon: How Russian Cyberpower Invaded the U.S.*, N.Y. TIMES (Dec. 13, 2016), https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html [https://perma.cc/6GU5-CF2K]; Tom Hamburger & Karen Tumulty, *WikiLeaks Releases Thousands of Documents About Clinton and Internal Deliberations*, WASH. POST (July 22, 2016), https://www.washingtonpost.com/news/post-politics/wp/2016/07/22/on-eve-of-democratic-convention-wikileaks-releases-thousands-of-documents-about-clinton-the-campaign-and-internal-deliberations/?utm_term=.1e13fbea91df [https://perma.cc/5QUF-8YA9].

2. *Democratic National Committee Apologizes to Sanders Over Emails*, REUTERS (July 25, 2016), http://www.reuters.com/article/us-usa-election-dnc-statement-idUSKCN1052BN [https://perma.cc/36UY-FE75].

3. Lipton et al., *supra* note 1; Evan Osnos et al., *Trump, Putin, and the New Cold War: What Lay Behind Russia's Interference in the 2016 Election—and What Lies Ahead?*, NEW YORKER 40, 52–53 (Mar. 6, 2017), http://www.newyorker.com/magazine/2017/03/06/trump-putin-and-the-new-cold-war [https://perma.cc/WN33-Z2UM].

4. Joe Uchill, *WikiLeaks Releases New DNC Emails Day Before Election*, HILL (Nov. 7, 2016), http://thehill.com/policy/cybersecurity/304648-wikileaks-releases-new-dnc-emails-suffers-cyberattack [https://perma.cc/8UWR-UFWX].

government.[5] Inept responses and inattention from the DNC staff and casual follow-up from the FBI allowed the hackers free reign in DNC networks for more than six months until senior DNC officials learned of the hacks and hired a private security firm to protect their systems.[6]

Meanwhile, reports that Russian intelligence agencies were responsible for hacking the DNC, disseminating the materials to WikiLeaks, and encouraging or reporting "fake news" on social media and in nonmainstream publications swirled around the last months of the presidential election campaign.[7] A hacker calling itself Guccifer 2.0 took credit for the leaks,[8] and WikiLeaks would not reveal its source.[9] Over the remainder of the summer and early fall of 2016, several cyber experts and private security firms publicly claimed that the DNC hack had been carried out by Russian intelligence operatives and was directly controlled by the Russian government.[10]

On October 7, the Department of Homeland Security (DHS) and the Office of the Director of National Intelligence (ODNI) issued a joint statement that the Intelligence Community was confident that the Russian government was responsible for the hack and publication of the materials in its attempt to "interfere with the US election process."[11] Although the joint

---

5. Lipton et al., *supra* note 1.

6. *Id.*

7. Sam Biddle, *Here's the Public Evidence Russia Hacked the DNC—It's Not Enough*, INTERCEPT (Dec. 14, 2016), https://theintercept.com/2016/12/14/heres-the-public-evidence-russia-hacked-the-dnc-its-not-enough/ [https://perma.cc/9UUZ-XERG]; Osnos et al., *supra* note 3.

8. Ellen Nakashima, *Cyber Researchers Confirm Russian Government Hack of Democratic National Committee*, WASH. POST (June 20, 2016), https://www.washingtonpost.com/world/national-security/cyber-researchers-confirm-russian-government-hack-of-democratic-national-committee/2016/06/20/e7375bc0-3719-11e6-9ccd-d6005beac8b3_story.html?utm_term=.ec7d861e243c [https://perma.cc/KX3A-FV6E].

9. Hannah Albarazi, *WikiLeaks' DNC Email Leak Reveals Off the Record Media Correspondence*, CBS: SF BAY AREA (July 22, 2016), http://sanfrancisco.cbslocal.com/2016/07/22/hilary-leaks-wikileaks-releases-democratic-national-committee-emails/ [https://perma.cc/M3SC-2SVB].

10. Lucian Kim, *Russian Security Expert Maintains Putin Was Behind DNC Hack*, NPR (Jan. 26, 2017), http://www.npr.org/2017/01/26/511851752/russian-security-expert-maintains-putin-was-behind-dnc-hack [https://perma.cc/3BP5-7875]; Ellen Nakashima, *Cybersecurity Firm Finds Evidence That Russian Military Unit Was Behind DNC Hack*, WASH. POST (Dec. 22, 2016), https://www.washingtonpost.com/world/national-security/cybersecurity-firm-finds-a-link-between-dnc-hack-and-ukrainian-artillery/2016/12/21/47bf1f5a-c7e3-11e6-bf4b-2c064d32a4bf_story.html?utm_term=.527e73a904ef [https://perma.cc/9JZ4-GE8U]; Sam Thielman, *DNC Email Leak: Russian Hackers Cozy Bear and Fancy Bear Behind Breach*, GUARDIAN (July 26, 2016), https://www.theguardian.com/technology/2016/jul/26/dnc-email-leak-russian-hack-guccifer-2 [https://perma.cc/9N7B-ZMLK].

11. Joint Statement from the Department of Homeland Security and Office of the Director of National Intelligence on Election Security, Director of National Intelligence (Oct. 7, 2016), https://www.dni.gov/index.php/newsroom/press-releases/215-press-releases-2016/1423-joint-dhs-odni-election-security-statement [https://perma.cc/4VXK-65F9]; Ellen Nakashima, *U.S. Government Officially Accuses Russia of Hacking Campaign to Interfere with Elections*, WASH. POST (Oct. 7, 2016), https://www.washingtonpost.com/world/national-security/us-government-

statement constituted an official attribution of the DNC hack to the Russian government, the statement provided no evidence to support its assessment.

On December 9, the Central Intelligence Agency (CIA) briefed members of Congress on an Intelligence Community assessment that concluded the Russian government conducted these cyber operations during the 2016 presidential election in order to assist the candidacy of Donald Trump.[12] According to the Intelligence Community assessment, intelligence assets with direct ties to the Kremlin provided the DNC e-mails as well as others from prominent Hillary Clinton supporters, such as campaign chairman John Podesta, to WikiLeaks.[13] Their conclusion that Russia was behind the hack was delivered with "high confidence."[14] The CIA briefing was not a formal assessment by the Intelligence Community because of minor disagreements among the agencies and because intelligence officials did not yet have specific intelligence demonstrating that Russian government officials directed the hackers to pass along their information to WikiLeaks.[15] On December 16, CIA Director John Brennan stated that the FBI and DNI supported the CIA's conclusion that the Russian government interfered in the election to assist the Trump candidacy and to attack U.S. democratic processes.[16]

President Barack Obama reportedly raised the issue of Russian hacking with Russian President Vladimir Putin in a side meeting during the G20 summit in China in September 2016.[17] President Obama claimed that Russian hacking stopped after his meeting with Putin.[18] The hacking may

---

officially-accuses-russia-of-hacking-campaign-to-influence-elections/2016/10/07/4e0b9654-8cbf-11e6-875e-2c1bfe943b66_story.html?utm_term=.655d3d88e3a6 [https://perma.cc/P8JE-T9MJ].

12. Adam Entous et al., *Secret CIA Assessment Says Russia Was Trying to Help Trump Win White House*, WASH. POST (Dec. 9, 2016), https://www.washingtonpost.com/world/national-security/obama-orders-review-of-russian-hacking-during-presidential-campaign/2016/12/09/31d6b300-be2a-11e6-94ac-3d324840106c_story.html?utm_term=.ccd9268101b8 [https://perma.cc/4LMY-LUU3].

13. *Id.*; David Sanger & Scott Shane, *Russian Hackers Acted to Aid Trump in Election, U.S. Says*, N.Y. TIMES (Dec. 9, 2016), https://www.nytimes.com/2016/12/09/us/obama-russia-election-hack.html [https://perma.cc/6CPG-6QJP].

14. Sanger & Shane, *supra* note 13.

15. Entous et al., *supra* note 12; *see also* Biddle, *supra* note 7 (detailing the limited evidence of links between the Russian government and WikiLeaks).

16. Adam Entous & Ellen Nakashima, *FBI in Agreement with CIA That Russia Aimed to Help Trump Win White House*, WASH. POST (Dec. 16, 2016), https://www.washingtonpost.com/politics/clinton-blames-putins-personal-grudge-against-her-for-election-interference/2016/12/16/12f36250-c3be-11e6-8422-eac61c0ef74d_story.html?utm_term=.fb5453a21996 [https://perma.cc/U8YY-NSSG].

17. Scott Detrow, *Obama on Russian Hacking: 'We Need to Take Action. And We Will'*, NPR (Dec. 15, 2016), http://www.npr.org/2016/12/15/505775550/obama-on-russian-hacking-we-need-to-take-action-and-we-will [https://perma.cc/Q2VB-URZL].

18. Louis Nelson, *Obama Says He Told Putin to 'Cut It Out' on Russia Hacking*, POLITICO (Dec. 16, 2016), http://www.politico.com/story/2016/12/obama-putin-232754 [https://perma.cc/QDX7-URNT].

have stopped, but the leaks from WikiLeaks continued, prompting President Obama to contact President Putin on the Moscow–Washington hotline on October 31.[19] Obama reportedly emphasized the gravity of the hacks to Putin, and he told Putin that "international law, including the law for armed conflict, applies to actions in cyberspace."[20] Meanwhile, the media reported on October 14 that President Obama ordered the CIA to develop options for a U.S. cyber response to the Russian efforts to interfere in the U.S. presidential election.[21] NBC News characterized the charge to the CIA as coming up with options for a retaliatory cyberattack against the Russian Federation.[22]

On December 29, the FBI and DHS released *Joint Analysis Report: GRIZZLY STEPPE—Russian Malicious Cyber Activity*.[23] The report reinforced the agencies' earlier conclusions that Russia was behind the DNC hack, and it provided new technical details about the methods used by Russian assets, including malware samples.[24] Still, the report offered little forensic evidence to confirm the government's attribution statement from October.[25]

Finally, on January 6, 2017, after briefing President Obama, President-elect Donald Trump, and members of the Senate and House in a classified session on behalf of the CIA, National Security Agency (NSA), and FBI, DNI James Clapper released an unclassified version of *Assessing Russian Activities and Intentions in Recent US Elections: The Analytic Process and Cyber Incident Attribution*.[26] Presumably the classified report included the details on Russian attribution. The public report concluded that Russia had conducted a large-scale cyber operation on the orders of President Vladimir

---

19. William M. Arkin, Ken Dilanian & Cynthia McFadden, *What Obama Said to Putin on the Red Phone About the Election Hack*, NBC NEWS (Dec. 19, 2016), http://www.nbcnews.com/news/us-news/what-obama-said-putin-red-phone-about-election-hack-n697116 [https://perma.cc/5CKG-G5XC].

20. *Id.*

21. William M. Arkin, Ken Dilanian & Robert Windrem, *CIA Prepping for Possible Cyber Strike Against Russia*, NBC NEWS (Oct. 14, 2016), http://www.nbcnews.com/news/us-news/cia-prepping-possible-cyber-strike-against-russia-n666636 [https://perma.cc/3VG4-N2YB].

22. *Id.*

23. U.S. DEP'T OF HOMELAND SEC. & FED. BUREAU OF INVESTIGATION, JOINT ANALYSIS REPORT: GRIZZLY STEPPE—RUSSIAN MALICIOUS CYBER ACTIVITY (2016), https://www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf [https://perma.cc/RGW3-QKYT] [hereinafter RUSSIAN MALICIOUS CYBER REPORT].

24. *Id.*; David E. Sanger, *Obama Strikes Back at Russia for Election Hacking*, N.Y. TIMES (Dec. 29, 2016), https://www.nytimes.com/2016/12/29/us/politics/russia-election-hacking-sanctions.html?_r=1 [https://perma.cc/3SKD-V4MT].

25. RUSSIAN MALICIOUS CYBER REPORT, *supra* note 23; Katie Bo Williams, *FBI, DHS Release Report on Russia Hacking*, THE HILL (Dec. 29, 2016), http://thehill.com/policy/national-security/312132-fbi-dhs-release-report-on-russia-hacking [https://perma.cc/4F57-AG84].

26. OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, BACKGROUND TO "ASSESSING RUSSIAN ACTIVITIES AND INTENTIONS IN RECENT US ELECTIONS": THE ANALYTIC PROCESS AND CYBER INCIDENT ATTRIBUTION 1 (2017) [hereinafter ODNI REPORT RUSSIAN INTERFERENCE].

Putin with the intention of "undermin[ing] public faith in the US democratic process."[27] Their objective was to "denigrate Secretary Clinton, and harm her electability and potential presidency" while helping Donald Trump win the election.[28] The report concluded "with high confidence that Russian military intelligence (General Staff Main Intelligence or GRU) used the Guccifer 2.0 persona and DCLeaks.com to release U.S. victim data obtained in cyber operations publicly and in exclusives to media outlets and relayed material to WikiLeaks."[29] In addition to hacking and releasing the e-mails and attachments, the Russian campaign included extensive use of social media and Internet trolls, along with propaganda on Russian-controlled media, including Russian TV channel RT America.[30]

Based on these reports, and more than five months after WikiLeaks published the DNC material, on December 29 the Obama administration announced a series of self-help retorsion[31] responses: sanctions on nine Russian intelligence agencies, companies, and individuals; expulsion of thirty-five intelligence assets in the United States; closure of two Russian compounds in the United States used by their intelligence agents; and release of information on Russian cyber activities designed to help defenders of cyber networks disrupt malicious Russian cyber activity.[32]

Despite the fact that the U.S. responses to the DNC hack were the strongest and most public ever by the United States in response to a State-sponsored cyber intrusion, reactions to the U.S. actions have been critical. In

---

27. *Id.* at ii.

28. *Id.*

29. *Id.* at ii–iii.

30. *Id.* at 2, 4, 6.

31. Retorsion consists of politically unfriendly but lawful responses to a State's actions that attempt to alter the State's conduct. Thomas Giegerich, *Retorsion*, *in* 8 THE MAX PLANCK ENCYCLOPEDIA OF PUBLIC INT'L LAW 976 (2012); *see also* Tom Ruys, *Sanctions, Retorsions and Countermeasures: Concepts and International Legal Framework*, *in* RESEARCH HANDBOOK ON UN SANCTIONS AND INTERNATIONAL LAW 1, 5 (Larissa van den Herik ed., 2016) (considering retorsion as a form of "self-help").

32. Office of the Press Sec'y, Statement by the President on Actions in Response to Russian Malicious Cyber Activity and Harassment (Dec. 29, 2016), https://obamawhitehouse.archives.gov/the-press-office/2016/12/29/statement-president-actions-response-russian-malicious-cyber-activity [https://perma.cc/XZ36-34S5]. On December 28, 2016, President Obama issued Exec. Order No. 13,757, allowing for the imposition of sanctions on individuals and entities determined to be responsible for tampering, altering, or causing the misappropriation of information with the purpose or effect of interfering with or undermining election processes or institutions. Taking Additional Steps to Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities, 82 Fed. Reg. 1 (Dec. 28, 2016). The Order amends an April 1, 2015 order, Exec. Order 13,694, "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities," which authorized the imposition of sanctions on individuals and entities determined to be responsible for or complicit in certain cyber-enabled activities that result in enumerated harms that are reasonably likely to result in, or have materially contributed to, a significant threat to the national security, foreign policy, or economic health and financial stability of the United States. Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities, 80 Fed. Reg. 18,077 (Apr. 1, 2015).

general, critics wondered why the United States waited so long and why we did not do more than impose those limited self-help measures. The responses were viewed as "too little, too late,"[33] or "confusing" and "weak,"[34] or simply "insufficient."[35]

Russian intelligence agencies have been penetrating sensitive computer networks inside the United States for more than twenty years.[36] President Obama was regularly briefed on escalating Russian hacking of government computers, but he declined to name the Russians publicly or impose sanctions, fearing an escalating cyberwar and needing Russian cooperation in negotiations over Syria.[37] When senior DNC executives first met with senior FBI officials in mid-June 2016, before any of the hacked materials had been published, DNC participants asked that the federal government formally blame the Russian government for the intrusions to emphasize to the American people that the hacks were foreign espionage, not routine hacking.[38] Nonetheless, the formal attribution of Russian government responsibility for the hacks did not come until October 7, and the limited sanctions were not announced until December 29.

Why did the United States wait so long to respond to the Russian intrusions? And why did we limit our responses to largely ineffectual self-help? The linchpin to understanding the timing and nature of the U.S. responses is a foundational component of cyber relations at international law—attribution. In common parlance, attribution means who is responsible, or assigning a cause to an action.[39] In the cyber domain, attribution means "identifying the agent responsible for the action."[40] Because the Internet facilitates anonymous communications and "was not designed with the goal of deterrence in mind,"[41] attribution of cyber intrusions can be challenging, particularly when the exploiters craft their intrusions to confound finding who is responsible.

---

33. Rebecca Crootof, *The DNC Hack Demonstrates the Need for Cyber-Specific Deterrents*, LAWFARE (Jan. 9, 2017), https://www.lawfareblog.com/dnc-hack-demonstrates-need-cyber-specific-deterrents [https://perma.cc/RU7U-5F4S].

34. Michael Morell, *Intelligence, Trump, Putin, and Russia's Long Game*, CIPHER BRIEF (Jan. 4, 2017), https://www.thecipherbrief.com/column/network-take/intelligence-trump-putin-and-russias-long-game-1091 [https://perma.cc/4P2E-PB39].

35. Maggie Penman & Ammad Omar, *Obama Announces Sanctions Against Russia In Response to Alleged Hacking*, NPR (Dec. 29, 2016), http://www.npr.org/sections/thetwo-way/2016/12/29/507430861/u-s-retaliates-against-russia-over-cyberattacks [https://perma.cc/FL8N-UJWJ].

36. Lipton et al., *supra* note 1.

37. *Id.*

38. *Id.*

39. David D. Clark & Susan Landau, *Untangling Attribution*, 2 HARV. NAT'L SEC. J. 531, 531 (2011).

40. *Id.*

41. *Id.*

Cyber attribution is more art than science and presents a multifaceted set of problems.[42] Law is only a part of the attribution calculus, and understanding the components of attribution is essential for shaping a legal and policy strategy to deter harmful cyber intrusions in the future.[43] As stated by former Assistant Attorney General for the National Security Division John Carlin,

> [A]ttributing activity on the Internet is challenging. Hackers often route their malicious traffic through third-party proxies they either rent or compromise. An attacker in Eastern Europe that uses a botnet of compromised computers in the Middle East to conduct a DDoS attack against a U.S. target creates a false narrative that actors located in the Middle East were responsible for that act. Even attributing an attack to the actual originating computer may be insufficient; we may know the machine used to execute a hack, but not the person or group that controlled it. Thus, technical investigation must often be supplemented by credible human intelligence. And all of this must be done quickly and consistently; attribution is of little use if it takes years and only identifies a small fraction of attackers.[44]

Attribution is a much discussed but underdeveloped part of international cyber law, particularly when States are the suspected responsible party. This Article will examine the treatment of attribution in the *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*[45] and critique the current state of international attribution law for cyber operations. In a nutshell, *Tallinn 2.0* fairly summarizes what amounts to substantially underdeveloped customary international law on attribution of cyber operations. Because cyber attribution remains challenging and often time-consuming when State responsibility is suspected, international law places States in an untenable posture in responding to cyber intrusions below the use of force level. I argue that States, including the United States, must make some difficult tradeoffs between secrecy and transparency and publicly identify some public-infrastructure "red lines" and attribution benchmarks that can help States create an international roadmap for deterrence of harmful

---

42. *Id.* at 324 (asserting that attribution "is not actually a technical issue at all, but a policy concern with multiple solutions depending on the type of technical issue . . . to be solved. . . . [S]olutions . . . lie outside the technical realm, and are instead in the space of law, regulation, multinational negotiation, and economics"); *id.* at 350.

43. *See* John P. Carlin, *Detect, Disrupt, Deter: A Whole-of-Government Approach to National Security Cyber Threats*, 7 HARV. NAT'L SEC. J. 391, 396–97 (2016) (describing attribution as an element of whole-of-government responses to cyber threats and the various parties involved in attribution).

44. *Id.* at 409 (footnotes omitted).

45. TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS (Michael N. Schmitt & Liis Vihul eds., 2017) [hereinafter TALLINN MANUAL 2.0].

cyber intrusions in the future. The United States should also make clear that it will employ a range of lawful responses to State-sponsored cyber intrusions, including commercial and trade-based tools.

I. *Tallinn 2.0* and Attribution

As was the case with the release of the *Tallinn Manual on the Law of Cyber Warfare* in 2013, expectations are high that the second project will coalesce disparate understandings of the international law of cyberspace.[46] Indeed, the *Tallinn Manual* provided much-needed confidence for States that international law applies in the cyber domain and supplied a framework for applying to cyberspace widely understood norms from kinetic conflict.[47] The *Tallinn Manual* also consisted in the main of what is at the core of *Tallinn 2.0*: the opinions of a distinguished International Group of Experts (IGE) on how international law norms apply to cyberspace. Where the first project applied the *jus ad bellum* and *jus in bello* to cyber incidents that cross a use-of-force threshold,[48] the objective of the second project was in some ways much more ambitious and arguably more important—examination of the international legal framework that applies to malevolent cyber operations that do not rise to the use-of-force level.[49]

Like the first book, *Tallinn 2.0* is intended as a restatement that reflects the law as it is (*lex lata*).[50] It also contains extensive commentary, providing the rationale for each rule. Still, *Tallinn 2.0* is not a treatise on international cyber law, nor does it establish new international law or represent the views of any States on their cyber operations. There could be no such treatise at this time because of insufficient State practice, a paucity of official State legal views, and a lack of consensus on norms. The Rules provided in *Tallinn 2.0* and their commentary are as a result necessarily general in nature, sometimes ambiguous, and do not necessarily reflect settled international law. These limitations are not in any way due to shortcomings in the *Tallinn 2.0* project.

---

46. *See* Michael J. Adams, *A Warning About Tallinn 2.0 . . . Whatever It Says*, LAWFARE (Jan. 4, 2017), https://www.lawfareblog.com/warning-about-tallinn-20-%E2%80%A6-whatever-it-says [https://perma.cc/3H3V-GHVQ] (discussing the positive reception of the *Tallinn Manual* and similarly heightened expectations for the *Tallinn Manual 2.0*); Colonel Gary Corn, Tallinn Manual 2.0—*Advancing the Conversation*, JUST SECURITY (Feb. 15, 2017), https://www.justsecurity.org/37812/tallinn-manual-2-0-advancing-conversation/ [https://perma.cc/7LF6-AJL7] (noting the large and diverse audience in attendance at the standing-room-only D.C. launch of the *Tallinn Manual 2.0*).

47. Adams, *supra* note 46.

48. TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE 4 (Michael N. Schmitt ed., 2013).

49. *See* William Banks, *The Role of Counterterrorism Law in Shaping* ad Bellum *Norms for Cyber Warfare*, 89 INT'L L. STUD. 157, 161 (2013), *reprinted in* ISRAEL YEARBOOK ON HUMAN RIGHTS 45 (Yoram Dinstein & Fania Domb eds., 2013) (noting that a majority of cyberattacks were left unregulated by the *Tallinn Manual*); TALLINN MANUAL 2.0, *supra* note 45, at 1.

50. TALLINN MANUAL 2.0, *supra* note 45, at 3.

Indeed, the Director and IGE did excellent work in compiling what amounts to a general summary of the rules and principles that apply to cyber operations below the use-of-force threshold.

Tallinn 2.0 offers a nuanced and elegant application of the basic principles of State responsibility to below-threshold cyber operations and their attribution. In some instances, *Tallinn 2.0* clarifies unsettled areas of the law. Yet *Tallinn 2.0* and its near-contemporaneous release with the U.S. response to the Russian DNC hack bring into sharp relief the fact that international law on State responsibility for cyber operations and their attribution fails to provide prescriptive norms that will help deter malicious cyber operations.

The increasing stakes of below-threshold cyber operations are well-illustrated by the DNC hack. The Russian government actions profoundly impacted a presidential election,[51] our nation's most important democratic institution. Without better legal rules of the road, harmful features of cyber exploitation will only grow in importance. As will be developed below, the combination of unclear and unrealistic attribution requirements, countermeasures law that is not compatible with cyber operations, and ineffectual and ill-timed retorsion responses to cyber intrusions that provide little or no deterrence enable gray zones in cyber law that only incentivize harmful cyber intrusions.

Tallinn 2.0 reminds us that the customary international law of State responsibility and attribution is largely drawn from the work of over a half century of the International Law Commission (ILC) and its Rules on State Responsibility. While not a treaty, and thus not binding on any nation, the ILC rules were commended to member States by the United Nations General Assembly in 2012 and have been cited repeatedly by courts, tribunals, and other bodies.[52] The unsurprising threshold point on State responsibility emphasized in Rule 14 of *Tallinn 2.0* is that "[a] State bears international responsibility for a cyber-related act that is attributable to the State and that constitutes a breach of an international legal obligation."[53] States care a great deal about cyber attribution precisely because the absence of attribution precludes State responsibility.[54]

---

51. *See* Richard Greene, *The Russian Hack Absolutely Affected the Outcome of the 2016 Election*, HUFFINGTON POST (Dec. 15, 2016), http://www.huffingtonpost.com/richard-greene/the-russian-hack-absolute_b_13656802.html [https://perma.cc/LS57-BSLQ] (arguing that Russian hacking had a palpable effect on the presidential election).

52. TALLINN MANUAL 2.0, *supra* note 45, at 79 n.112.

53. *Id.* at 84 (Rule 14).

54. *See, e.g.*, Phosphates in Morocco (It. v. Fr.), Preliminary Objections, 1938 P.C.I.J. (ser. A/B) No. 74, at 10, 28 (June 14) ("This act being attributable to the State and described as contrary to the treaty right of another State, international responsibility would be established immediately as between the two States."); United States Diplomatic and Consular Staff in Tehran (U.S. v. Iran), Judgment, 1980 I.C.J. 73, ¶¶ 29–30 (May 24).

Rules 15–18 of *Tallinn 2.0* summarize the customary international law of attribution of cyber operations in nuanced terms. Rule 15 states that "[c]yber operations conducted by organs of a State, or by persons or entities empowered by domestic law to exercise elements of governmental authority, are attributable to the State."[55] Rule 15 may be reduced to an admonition that States are responsible for cyber-related acts of their own officials, agents, contractors, non-State actors, and other States to the extent they actually control the operations. Some explanation helps place application of the Rule in a few less obviously State-controlled settings.[56] One useful example from the IGE narrative concerns "spoofing," the practice of a representative of a State impersonating another State or its IP addresses and thereby feigning identity and sometimes its location.[57] Particularly when a cyber intrusion demands an immediate response from the victimized State, spoofing can completely flummox existing international law on attribution. The IGE counsels assessing the context of each such situation and expresses hope that patterns of cyber behavior, human intelligence, and a history of diplomatic relations between States will ameliorate the impacts of spoofing.[58]

Rule 16 states that "[c]yber operations conducted by an organ of a State that has been placed at the disposal of another State are attributable to the latter when the organ is acting in the exercise of elements of governmental authority of the State at the disposal of which it is placed."[59] The same practical application of State responsibility provides the basis for Rule 17, which states that "[c]yber operations conducted by a non-State actor are attributable to a State when: (a) engaged in pursuant to its instructions or under its direction or control; or (b) the State acknowledges and adopts the operations as its own."[60] In other words, States do not escape legal responsibility for internationally wrongful acts by perpetrating them through proxies. The extension of State responsibility to private actors that are acting under the direction and control of the State drives this Rule, which embraces the "effective control" formulation from the International Court of Justice in its *Nicaragua* and *Genocide* judgments.[61] One wrinkle that distinguishes attribution of non-State actors to States is that the *ultra vires* acts of non-State actors are generally not attributable to the State.[62] An example illustrates the

55. TALLINN MANUAL 2.0, *supra* note 45, at 87 (Rule 15).

56. *Id.* at 88–90.

57. *Id.* at 91.

58. *Id.* at 92.

59. *Id.* at 93 (Rule 16).

60. *Id.* at 94 (Rule 17).

61. Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, ¶ 115 (June 27); Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosn. & Herz. v. Serb. & Montenegro), Judgment, 2007 I.C.J. 108, ¶ 400 (Feb. 26).

62. TALLINN MANUAL 2.0, *supra* note 45, at 97.

limits of the principle of direction and control: a State instructs a non-State actor to introduce malware into another State's government networks and the non-State actor misappropriates the malware to target a third state. There is no attribution to the State because the non-State actor implemented the instruction in a way that was *ultra vires*.[63]

Finally, Rule 18 maintains that:

> [A] State is responsible for: (a) its aid or assistance to another State in the commission of an internationally wrongful act when the State provides the aid or assistance knowing of the circumstances of the internationally wrongful act and the act would be internationally wrongful if committed by it; (b) the internationally wrongful act of another State it directs and controls if the direction and control is done with knowledge of the circumstances of the internationally wrongful act and the act would be internationally wrongful if committed by it; or (c) an internationally wrongful act it coerces another State to commit.[64]

This rule simply imports noncyber considerations of State responsibility to the cyber domain.

II. Complying with International Law on Attribution: The Russia DNC Hack

Despite the persuasive criticisms of the U.S. responses to the Russian hack on the DNC, the U.S. government responses were carefully limited to comply with the current state of the law permitting only self-help responses under the international law of State responsibility and attribution. It bears emphasizing that attribution is a necessary precondition before responding to State-sponsored cyber intrusions. As the private security firm findings, intermediate agency reports, congressional briefings, and White House statements indicated, Russian involvement was suspected early on, before the publication of the materials began. However, the attribution report that the highest levels of the Russian government, including President Putin, directed and controlled the cyber hacking, exfiltration, and dissemination of private data in the United States was not delivered to President Obama's desk until much later.[65] Even then, rather than public attribution from the President, the White House ordered a relatively low-key release of the DHS/ODNI statement attributing the attacks to Russia on October 7.

As the January 6, 2017, *Assessing Russian Activities and Intentions* report indicated,

---

63. *Id.* at 98.
64. *Id.* at 100 (Rule 18).
65. Lipton et al., *supra* note 1.

> [a]n assessment of attribution usually is not a simple statement of who conducted an operation, but rather a series of judgments that describe whether it was an isolated incident, who was the likely perpetrator, that perpetrator's possible motivations, and whether a foreign government had a role in ordering or leading the operation.[66]

High confidence in State responsibility for the DNC hack required multiple agencies working their intelligence sources and methods, analysts' reviews of the evidence and judgments made on the evidence, and collective Intelligence Community judgments based on previous experience and the materials collected surrounding this case. Indeed, a unanimous Intelligence Community determination that military intelligence officials in the Russian government directed that the purloined e-mails be delivered to WikiLeaks was not achieved until sometime in December. In this instance attribution was aided by a parallel recent history of Russian hackers pursing political targets in Ukraine, Georgia, Estonia, and at North Atlantic Treaty Organization (NATO) installations.[67] A private security firm hired by the DNC also attributed the hacks to Russian State hackers.[68] That the Obama administration delayed formal State attribution to October, downplayed the announcement, and delayed implementation and a public statement of sanctions until the end of December was likely due to a combination of fear of escalation, a desire not to alienate Russia during Syria negotiations, and an expectation that Hillary Clinton would win the election in any case. Clearly, the Obama administration would have been reluctant to publicly announce sanctions against Russian hacking of the DNC and Clinton campaign before the election because of the appearance of punishing the Russians to benefit the Democratic candidate. In June or July, the sanctions that appeared too little, too late in December would have come across as aggressive and partisan.

Retired General and former NSA and CIA Director Michael Hayden helped place the U.S. response to the DNC hack in context by reminding us that the United States has only rarely officially attributed a malicious cyber operation to another State—China following widespread corporate espionage in 2014[69] and North Korea following the Sony hack in 2014[70]—and that when the United States makes such a public declaration "you can take it to the

66. ODNI REPORT RUSSIAN INTERFERENCE, *supra* note 26, at 2.

67. Lipton et al., *supra* note 1.

68. *Id.*

69. Robert Chesney, *DOJ's Summary of the Charges in the Chinese Economic Espionage Case*, LAWFARE (May 19, 2014), https://www.lawfareblog.com/dojs-summary-charges-chinese-economic-cyberespionage-case [https://perma.cc/KFN2-XYY4].

70. Herb Lin, *Learning from the Attack Against Sony*, LAWFARE (Jan. 23, 2015), http://www.lawfareblog.com/learning-attack-against-sony [https://perma.cc/6ZKP-5ZA2].

bank."[71] General Hayden also opined that Russia effectively "weaponized the information" they exfiltrated in an attempt to erode confidence in our democratic system.[72] Although General Hayden was not specifically critical of the Obama administration's actions in this instance, he suggested that other more aggressive geopolitical measures would have been appropriate.[73]

Retired Admiral James Stavridis, former head of NATO forces in Europe, offered a series of potential responses to the Russian DNC hack that he maintained would underscore U.S. determination to "respond with a firm hand."[74] Among other things, Admiral Stavridis argued that "the United States could use its own offensive cyber-tools to punish Russian hackers by knocking them off-line or even damaging their hardware."[75] Acknowledging that some would object that such a response may escalate the conflict, Admiral Stavridis admitted that "[t]he burden of proof for attribution would be higher" if we responded as above and "would be viable only if Washington had definitive information on the command and control centers that launched the hacking activity."[76] Admiral Stavridis's proposal to disconnect the hackers from Internet connectivity is likely not prohibited by international law unless doing so would require some kind of entry into the hackers' systems. Damaging the hackers' hardware would in all likelihood, however, be characterized as a forbidden use of force at international law.[77] Admiral Stavridis wisely recognized that any response to a responsible State requires attribution to that State. Yet Admiral Stavridis overstated international law attribution requirements. Applying the Rules on State responsibility and attribution compiled in *Tallinn 2.0*, there is no burden of proof or requirement that there exists "definitive information" on attribution. Although wise as a matter of policy, the failure to offer persuasive evidence of State attribution is not wrongful legally.

---

71. *Gen. Hayden on U.S. Response to Russian DNC Hack*, WALL ST. J. (Dec. 7, 2016), http://www.wsj.com/video/gen-hayden-on-us-response-to-russian-dnc-hack/54D57FC3-D99E-4864-B9C7-EE948791158A.html [https://perma.cc/GAW2-UXDC].

72. *Id.*

73. *Id.*

74. James Stavridis, *How to Win the Cyberwar Against Russia*, FOREIGN POLICY (Oct. 12, 2016), http://foreignpolicy.com/2016/10/12/how-to-win-the-cyber-war-against-russia/ [https://perma.cc/WSX2-69L7].

75. *Id.*

76. *Id.*

77. *See* 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, 208–09 (2002) (arguing that cyberattacks against a nation's critical infrastructure should constitute an act of force giving rise to a right of proportionate self-defense under the United Nations Charter); TALLINN MANUAL 2.0, *supra* note 45, at 28 (noting that "interference with an object enjoying sovereign immunity constitutes a violation of international law," and that "[i]nterference includes, but is not limited to, activities that damage the object").

It is important to place the DNC hack in the larger context of cyber intrusions. The DNC hack clearly was not an armed attack or use of force.[78] Below the use of force threshold, States are responsible for a "cyber-related act . . . that constitutes a breach of an international legal obligation."[79] The breach may be a violation of a treaty or customary international law, or other "general principles of law."[80] Outside an armed conflict and below the use-of-force threshold, cyber intrusions constitute an international law breach by violating the prohibition on intervention.[81] The prohibition on intervention, based on the international law principle of sovereignty, forbids coercive intervention by cyber means.[82] *Tallinn 2.0* affirms that State-on-State cyber acts that are "detrimental, objectionable, or otherwise unfriendly"[83] are not breaches and do not trigger State responsibility. However, physical damage or injury is not necessary to render a cyber operation an internationally wrongful act "unless damage is an element of breach of the primary rule."[84] Nor is intent to cause harm generally a requirement of an internationally wrongful act.[85] Violations of domestic law cannot be the basis for an internationally wrongful act,[86] because the existence of a legal obligation is determined solely by international law.[87]

Based on the publicly available evidence, the DNC hack probably was not an unlawful intervention. In a November 2016 speech, Department of State Legal Adviser Brian Egan opined that "a cyber operation by a State that interferes with another State's ability to hold an election or that manipulates a State's election results would be a clear violation of the rule of non-intervention."[88] The *Tallinn 2.0* experts similarly suggest that remotely altering electronic ballots to manipulate election results constitutes an unlawful intervention.[89]

The core requirement of a prohibited intervention is coercion.[90] As confirmed by the International Court of Justice in the *Nicaragua* judgment,

---

78. *See* TALLINN MANUAL 2.0, *supra* note 45, at 107, 364–65 (discussing cyber operations that qualify as "armed attacks" and "uses of force").

79. *Id.* at 84 (Rule 14).

80. *Id.* at 84.

81. *Id.* at 312.

82. *Id.* at 313.

83. *Id.* at 85.

84. *Id.* at 86.

85. *Id.*

86. *Id.*

87. G.A. Res. 56/83, Articles on State Responsibility, art. 3 (Jan. 28, 2002).

88. Brian J. Egan, Remarks on International Law and Stability in Cyberspace at Berkeley Law School (Nov. 10, 2016), https://www.justsecurity.org/wp-content/uploads/2016/11/Brian-J.-Egan-International-Law-and-Stability-in-Cyberspace-Berkeley-Nov-2016.pdf [https://perma.cc/4DXB-9TNH].

89. TALLINN MANUAL 2.0, *supra* note 45, at 313.

90. *Id.* at 317.

"the element of coercion . . . forms the very essence of [] prohibited intervention."[91] As understood in *Tallinn 2.0*, coercion "is not limited to physical force, but rather refers to an affirmative act designed to deprive another State of its freedom of choice . . . to force that State to act in an involuntary manner or involuntarily refrain from acting in a particular way."[92] A January 2017 memorandum from the General Counsel of the Department of Defense to the Combatant Commands and other senior military and civilian lawyers in the Pentagon affirmed coercion as a prerequisite means for unlawful intervention, and concluded that military cyber activities that fall below the use of force threshold and do not violate the nonintervention principle are "largely unregulated by international law at this time."[93]

Measured against those customary international criteria, the Russian hack likely was not an internationally wrongful act. The Russians exfiltrated and disseminated private information but did not tamper with voting machines or change votes. According to the traditional measures, there was no coercion and no unlawful intervention. We should temper our confidence in this coercion analysis, however, because state practice and resulting customary international law are based on examples from kinetic conflicts. The analogies to cyber are not necessarily conclusive. If we extrapolate from General Hayden's metaphor that the Russians effectively "weaponized the information" they stole for the purpose of eroding confidence in the U.S. democratic system, the Russian exfiltration looks more coercive. In any case, the United States could not respond to Russia until it attributed State responsibility for the attacks.

III. The International Law Problems with Countermeasures in Cyber

For the sake of argument, assume that the Russian DNC hack was an unlawful intervention. What could the United States have done in response? Admiral Stavridis appeared to propose what international law refers to as countermeasures. Countermeasures are responses, whether cyber in nature or not, below the use-of-force threshold designed to prevent or mitigate a perpetrator State from continuing its unlawful cyber intervention.[94] Though

---

91. Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, ¶ 205 (June 27).

92. TALLINN MANUAL 2.0, *supra* note 45, at 317.

93. Dep't of Def., Memorandum for Commanders of the Combatant Commands, International Law Framework for Employing Cyber Capabilities in Military Operations (2017) (on file with author). The Memorandum acknowledges that the "exact contours of cyber activities that might violate the principle of non-intervention are not clear, and will continue to develop with state practice over time." *Id.*

94. *See* TALLINN MANUAL 2.0, *supra* note 45, at 111 ("Only available in response to internationally wrongful acts, countermeasures are actions or omissions by an injured State directed against a responsible State that would violate an obligation owed by the former to the latter but for

short of a use of force, countermeasures would be unlawful themselves but for the purpose of stopping the intrusion.[95] Because they respond to an internationally wrongful act, countermeasures require prior attribution and notice to the offending State that the victim State knows the source of the cyber intrusion.[96] International law also requires giving the aggressor State a chance to forbear.[97] In addition, the countermeasures must be proportional to the original intrusion[98] and they must have as their purpose "induc[ing] compliance with international law."[99] Punitive countermeasures are forbidden.[100]

In October 2014, the United States made a public submission[101] to the United Nations Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security, a group focused in recent years on identifying legal norms in cyberspace. Among other subjects, the U.S. submission noted the legal limits on exercising countermeasures in cyberspace, including the requirement of the injured State to call on the responsible State to comply with its international obligations before launching cyber countermeasures, except in exigent circumstances.[102]

Even if the Russian operation was an unlawful intervention, the long lag time between the hack and a confident State attribution rendered countermeasures unavailable. Countermeasures are designed to persuade the perpetrator to stop its unlawful actions, not as punishment or escalation. Putting aside the specifics of the DNC hack, cyber intrusions below the use-of-force level are normally quick-hitting, allowing insufficient time for the countermeasures regime to play out in a State-on-State setting. Following the countermeasures requirements of notice to the offender and giving them a chance to refuse to stop their actions is unrealistic in the cyber environment.

Although the technological aspects of attribution have advanced considerably in recent years,[103] settling on State responsibility involves more

---

qualification as a countermeasure."); Nicar. v. U.S., 1986 I.C.J. 14, ¶ 249; Gabčíkovo-Nagymaros Project (Hung. v. Slovk.), 1997 I.C.J. 7, ¶¶ 82–83 (Sept. 25).

95. TALLINN MANUAL 2.0, *supra* note 45, at 111.

96. *Id.* at 120.

97. *Id.*

98. *Id.* at 127 (Rule 23).

99. *Id.* at 112.

100. *Id.* at 124.

101. Applicability of International Law to Conflicts in Cyberspace, 2014 DIGEST OF U.S. PRACTICE IN INTERNATIONAL LAW, ch. 18, § A(3), at 13, https://www.state.gov/documents/organization/244486.pdf [https://perma.cc/5VDX-2M7X] [hereinafter 2014 U.S. SUBMISSION TO THE GGE].

102. *Id.* at 20.

103. *See* Herbert Lin, *Attribution of Malicious Cyber Incidents: From Soup to Nuts*, J. INT'L AFFAIRS ONLINE (Mar. 9, 2017), https://jia.sipa.columbia.edu/attribution-malicious-cyber-incidents [https://perma.cc/2CTP-8Q6Z] (synthesizing various discussions of attribution, specifically as it relates to malicious cyber acts).

than technical attribution of the offending machine, or even the operator of the machine. If a State victimized by an internationally wrongful cyber intrusion engages in countermeasures too early and is wrong about State attribution, the victimized State has committed an internationally wrongful act.[104] If the victim State waits until it has high confidence in State responsibility for the intrusion, any countermeasures that are implemented may be construed as punishment, forbidden under international law.[105] As a result, cyber deterrence may be undermined because the limited available self-help retorsion responses to an intrusion like the DNC hack are weak and unlikely to deter similar cyber intrusions in the future.

Attribution can mean different things depending on a State's objectives. Attribution of malicious cyber activity can trace to a machine, to one or more persons operating the machine that initiates the cyber intrusion, and to a person or entity that is found to be ultimately responsible for that activity.[106] Attribution is determined by a wide range of facts, including technical forensics, human intelligence, signals intelligence, history, and diplomatic relations, among others.[107] The declassified *Background to "Assessing Russian Activities and Intentions in Recent US Elections"* reminds us that intelligence analysis of cyber intrusions seeks "to reduce the uncertainty surrounding foreign activities, capabilities, or leaders' intentions. This objective is difficult to achieve when seeking to understand complex issues on which foreign actors go to extraordinary lengths to hide or obfuscate their activities."[108] The Intelligence Community assessment reflects "a series of judgments that describe whether [the intrusion] was an isolated incident, who was the likely perpetrator, the perpetrator's possible motivations, and whether a foreign government had a role in ordering or leading the operation."[109]

Recognizing that customary international law has not developed a set of understandings or recognized State practice on what level of attribution is acceptable or necessary for establishing State responsibility for cyber actions, the IGE concluded that "States may agree between themselves to a rule of responsibility specific to a cyber act or practice."[110] The result would be *lex specialis* to the extent the rule conflicts directly with general principles of State responsibility.[111] Discerning no such rules or understandings among

104. TALLINN MANUAL 2.0, *supra* note 45, at 118–20.

105. *Id.* at 116.

106. Clark & Landau, *supra* note 39, at 532.

107. *See* Carlin, *supra* note 43, at 396–97 (discussing the various experts required for the complex attribution analysis).

108. ODNI REPORT RUSSIAN INTERFERENCE, *supra* note 26, at 1.

109. *Id.* at 2.

110. TALLINN MANUAL 2.0, *supra* note 45, at 80.

111. As per the traditional legal maxim "specific law prevails over general law." *See Generalia Specialibus Non Derogant*, BLACK'S LAW DICTIONARY (10th ed. 2014) ("The doctrine holding that

States today, the IGE acknowledged the "uncertainty as to the attribution of cyber operations" and agreed "that as a general matter, States must act as reasonable States would in the same or similar circumstances when considering responses to them."[112] The IGE elaborated in this way:

> Reasonableness is always context dependent. It depends on such factors as, *inter alia*, the reliability, quantum, directness, nature (e.g., technical data, human intelligence), and specificity of the relevant available information when considered in light of the attendant circumstances and the importance of the right involved. These factors must be considered together. Importantly in the cyber context, deficiencies in technical intelligence may be compensated by, for example, the existence of highly reliable human intelligence.[113]

Reasonableness may also take into account "the severity of the cyber operations being directed against the State and the robustness of any possible response."[114] The IGE suggested that "as a general matter the graver the underlying breach . . . , the greater the confidence ought to be in the evidence relied upon by a State considering a response[115] . . . because the robustness of permissible self-help responses . . . grows commensurately with the seriousness of the breach."[116] At the same time, "the severity of the cyber operations directed at the injured State"[117] matters. A State confronted with "low-level cyber operations that are merely disruptive" may be expected to amass more evidence for attribution than a State victimized by "devastating cyber operations and needing to respond immediately to terminate them."[118] To put it slightly differently, the IGE acknowledged that all attribution judgments that determine State responsibility are necessarily accompanied by some measure of uncertainty. Because there is no accepted State practice, nor international agreement or domestic law on how much evidence suffices for attribution of State responsibility, the attribution bar is at present set very low by international law.

Nor is the failure of a State to provide persuasive proof of attribution itself an internationally wrongful act. There are no burdens of proof or

---

general words in a later statute do not repeal an earlier statutory provision dealing with a special subject."); TALLINN MANUAL 2.0, *supra* note 45, at 81.

112. TALLINN MANUAL 2.0, *supra* note 45, at 81.

113. *Id.* at 81–82.

114. *Id.* at 82.

115. *Id.* In support of its position, the IGE cited Oil Platforms (Iran v. U.S.), Judgment, 2003 I.C.J. 161, ¶ 33 (Nov. 6) (separate opinion of Judge Higgins); Corfu Channel (U.K. v. Alb.), Judgment, 1949 I.C.J. 4, 17 (Apr. 9); Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosn. & Herz. v. Serb. & Montenegro), Judgment, 2007 I.C.J. 108, ¶¶ 209–10 (Feb. 26); Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Croat. v. Serb.), 2015 I.C.J. General List No. 118, ¶ 178 (Feb. 3).

116. TALLINN MANUAL 2.0, *supra* note 45, at 82.

117. *Id.*

118. *Id.*

additional legal criteria for establishing attribution. The 2015 United Nations Group of Governmental Experts (GGE) report noted that accusations of wrongful acts by States "should be substantiated,"[119] but the GGE gave no indication of which or how much evidence would suffice or even count. The United States' view, articulated by State Department Legal Adviser Brian Egan in November 2016, is that "a State acts as its own judge of the facts and may make a unilateral determination with respect to attribution of a cyber operation to another State. . . . [T]here is no international legal obligation to reveal evidence on which attribution is based prior to taking appropriate action."[120]

States are likewise not obligated to publicly provide evidence of attribution when responding to another State's cyber intrusions.[121] While the IGE acknowledged the value in such a disclosure requirement, they found insufficient State practice and *opinio juris* to recognize "an established basis under international law for such an obligation."[122] The IGE noted that the highly classified nature of such attribution assessments is the primary reason for the absence of customary international law on this important point.[123] The October 2014 U.S. submission to the GGE is consistent with the IGE on all of these points.[124]

IV. Assessing the State of Attribution Law

Over time, an international consensus may develop on the minimum level of involvement needed to declare that a State is legally responsible for a cyber operation. But we are not there yet. In working to attribute an intrusion to a human perpetrator or an ultimately responsible State, technical forensics by themselves are generally inconclusive,[125] and the information they provide must often be combined with other sources to be genuinely useful.[126] The fact that attribution judgments draw on many different sources of information has one major temporal implication—early judgments made with less information are generally less believable than later judgments made

---

119. Rep. of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, ¶ 24, U.N. Doc. A/70/174 (July 22, 2015).

120. Egan, *supra* note 88, at 19.

121. TALLINN MANUAL 2.0, *supra* note 45, at 83.

122. *Id.*

123. *Id.*

124. *See* Michael Schmitt, *U.S. Transparency Regarding International Law in Cyberspace*, JUST SECURITY (Nov. 15, 2016), https://www.justsecurity.org/34465/transparency-international-law-cyberspace/ [https://perma.cc/UCY4-5VBT].

125. *See* Thomas Rid & Ben Buchanan, *Attributing Cyber Attacks*, 38 J. STRATEGIC STUD. 4, 7 (2015) (noting that using technical forensics to attribute a cyber attack to a specific actor is more of an art than a science).

126. *See* Lin, *supra* note 103 (observing that the duration of the Sony investigation was due in part to an absence of other sources).

with more information. Continuing investigation may reveal additional useful information, which may (or may not) reinforce attribution judgments made earlier.

The lucid analysis by the IGE in *Tallinn 2.0* affirms that international law does not incentivize careful and thorough efforts at attribution in cyber operations. For example, there is no incentive at international law for a State planning self-help retorsion to be certain of State responsibility and refrain from responding to a cyber intrusion before all the facts are in so long as it does not engage in an internationally wrongful act. Meanwhile, the fact that attribution of State responsibility for an internationally wrongful cyber intervention may take a long time and thus defeat the countermeasures option creates a particularly unhelpful set of choices—to respond with countermeasures based on incomplete evidence and risk making a mistake that constitutes an internationally wrongful act or wait to implement countermeasures only after there is solid evidence of State responsibility. By such time, the original victimized State will have engaged in an internationally wrongful act because the international law criteria for a countermeasure are not satisfied and the putatively defensive measures will be seen as an attack.

One positive development in the attribution landscape in the past several years is the increasing involvement of private-sector firms in rendering attribution judgments. The 2015 Department of Defense Cyber Strategy notes that security firms reporting on attribution "can play a significant role in dissuading cyber actors from conducting attacks in the first place" and states that "[t]he Defense Department will continue to collaborate closely with the private sector and other agencies of the U.S. government to strengthen attribution. This work will be especially important for deterrence as activist groups, criminal organizations, and other actors acquire advanced cyber capabilities over time."[127]

For example, in February 2013 Mandiant issued an extensive report on Chinese cyber espionage that relied on detailed evidence of Chinese government attribution.[128] Mandiant found with a high degree of confidence that a specific unit of the People's Liberation Army (PLA) perpetrated hacks on many of the targeted industries in the United States, after first identifying the particular machines and operators involved in the espionage.[129] The Mandiant work helped pave the way for the May 2014 indictments by the

127. DEP'T OF DEF., THE DEPARTMENT OF DEFENSE CYBER STRATEGY 12 (2015), https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf [https://perma.cc/2LS5-CPCZ].

128. MANDIANT, APT1: EXPOSING ONE OF CHINA'S CYBER ESPIONAGE UNITS 2 (2013), https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf [https://perma.cc/Q4WP-VQDG].

129. *Id.* at 3–7. Mandiant acknowledged the "unlikely possibility" that a group of private hackers had engaged in espionage similar to that conducted by the PLA. *Id.* at 6.

Justice Department of five PLA members on economic espionage charges.[130] In another example, after senior DNC executives learned from FBI officials that they had been hacked, the DNC hired CrowdStrike, a cybersecurity firm, to rebuild its computer security.[131] Within a day, CrowdStrike advised its client that the hacks originated in Russia.[132] Several other prominent examples of private security firms' involvement in attribution of cyber intrusions by States are noted below.[133]

On the one hand, private firms' cases for attribution of State responsibility are speculative. They can provide computer forensics and, at times, identify the operators of perpetrator machines.[134] But they lack the authority and means to collect the human intelligence necessary to reliably find State attribution. There is a big difference between saying that Russians hacked and Russia hacked. In addition, the companies have a self-interested stake in marketing their brand and encouraging further work on Internet security. The companies may lack the independence and rigor that we expect of government intelligence work.[135] On the other hand, private security firms can provide a public accounting of responsibility for malicious cyber actions with analytical and collection resources beyond those employed by States. The unclassified nature of their reports both provides a transparent airing of attribution and takes the pressure off government to share its sources and methods while allowing government to avoid responsibility for the attribution judgment.

From a policy perspective, the implications of these developments for cyber attribution are coming into sharper focus. A determination of

---

130. Ellen Nakashima, *Following U.S. Indictments, China Shifts Commercial Hacking Away from Military to Civilian Agency*, WASH. POST (Nov. 30, 2015), https://www.washingtonpost.com/world/national-security/following-us-indictments-chinese-military-scaled-back-hacks-on-american-industry/2015/11/30/fcdb097a-9450-11e5-b5e4-279b4501e8a6_story.html?utm_term=.d21182d3328f [https://perma.cc/8UU5-X6H9].

131. Lipton et al., *supra* note 1.

132. *Id.*

133. *See* CROWDSTRIKE, CROWDSTRIKE INTELLIGENCE REPORT: PUTTER PANDA (2014), https://cdn0.vox-cdn.com/assets/4589853/crowdstrike-intelligence-report-putter-panda.original.pdf [https://perma.cc/2FPF-GQ53] (concluding that Unit 61486 in the PLA was likely responsible for the cyber theft of trade secrets against entities in the satellite, aerospace, and communication industries); FIREEYE, APT28: A WINDOW INTO RUSSIA'S CYBER ESPIONAGE OPERATIONS? (2014), http://www2.fireeye.com/rs/fireye/images/rpt-apt28.pdf [https://perma.cc/BSG7-8WME] (presenting evidence that Russia was involved in espionage against private-sector and government actors); NOVETTA, OPERATION SMN: AXIOM THREAT ACTOR GROUP REPORT (2014), http://www.novetta.com/wp-content/uploads/2014/11/Executive_Summary-Final_1.pdf [https://perma.cc/UTX3-ESS6] (contending that the Chinese government was likely involved in cyber espionage against several private companies, governments, journalists, and prodemocracy groups).

134. *See* Biddle, *supra* note 7 (discussing a private security firm's forensic findings following the DNC hack).

135. Lin, *supra* note 103 n.62.

attribution is rarely definitive, and will usually be hedged with some degree of uncertainty.

The necessary degree of confidence in an attribution judgment depends on the nature of the malicious activity being attributed and the action that is contemplated in its aftermath. The audience that an attribution judgment seeks to persuade has a significant impact on how subsequent aspects of the attribution process unfold. The *Tallinn 2.0* experts recognize these variables and their importance.

V. The National Security Implications of the International Law on Attribution

States want to set responsibility for malicious actions in the cyber domain so that governments can decide what action to take in response and against whom. Technology may be sufficient for attribution in cyber if governments want to stop or impact the machine that is causing the harm. If instead governments want to prosecute a cyber perpetrator, different attribution from different sources will likely be required. Knowing the machine doesn't necessarily lead to the operator. If the goal is to fix State responsibility more may be required.

The sources and methods pursued to determine attribution in national security cyber cases are in some ways different and in some ways like those used in law enforcement. Much of the evidence of attribution is off-line and involves traditional interviews and the examination of equipment.[136] Much of the sleuthing is also vulnerable to efforts by adversaries to thwart or slow down investigations, often through cyber means such as spoofing on location and identity.

How much evidence of attribution is enough? As reflected in the commentary in *Tallinn 2.0*, international law requires a granular analysis, taking into account "the reliability, quantum, directness, nature (e.g., technical data, human intelligence), and specificity of the relevant available information when considered in light of the attendant circumstances and the importance of the right involved."[137] A State merely encouraging a non-State actor to undertake a malicious cyber intrusion is not sufficient for State responsibility.[138] In this respect, the nuance and detail offered in *Tallinn 2.0* is extremely valuable, showing how judicial decisions and analysis from customary international law sources can help in determining attribution.

The time it takes to produce an attribution judgment with high confidence can significantly impact the lawful responses to cyber intrusions. In some circumstances mistaken attribution can lead to an unlawful response

136. Carlin, *supra* note 43, at 414–15.

137. TALLINN MANUAL 2.0, *supra* note 45, at 82.

138. *Id.* at 97.

even if the victimized State made a reasonable determination of attribution and implemented countermeasures.[139] In national security contexts, the IGE opined that "as a general matter the graver the underlying breach . . . the greater the confidence ought to be in the evidence relied upon by a State considering a response."[140] More robust responses require more evidence, and the more severe the injury to the victim State, the less certain of attribution the State needs to be.[141] Similarly, low-level cyber intrusions that are disruptive but not destructive place victimized States "in a position to accumulate more evidence for attribution," suggesting a case-by-case evaluation of required attribution.[142]

Apart from the substantive attribution criteria, international law is unlikely to play an important role in contributing predictability and stability in cyberspace relations among States without greater transparency within and among States on their cyber norms and practices than now exists. Customary international law, after all, develops from a consistent practice of States followed out of a sense of legal obligation.[143] When States articulate their views on how international law applies to cyber operations, such public statements increase expectations of State behavior and thus contribute to greater predictability and stability in cyber operations.[144] Instances such as the Russian attempts to interfere with the 2016 election provide an opportunity for the United States to clearly and unequivocally delineate red lines, reinforced by a set of lawful responses that would follow their breach. That the Obama administration equivocated, delayed attribution, and then delayed ineffectual sanctions did not serve those important international law objectives.

Reacting in December 2016 to the Obama administration's relative public silence on the Russian DNC hacks, former acting director of the CIA Michael Morell opined that "[a] foreign government messing around in our elections is . . . the political equivalent of 9/11."[145] Morell pointed out that North Korea, China, and Iran are watching the U.S. reaction to the Russian

---

139. *Id.* at 82–83.

140. *Id.* at 82; *see also* Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosn. & Herz. v. Serb. & Montenegro), Judgment, 2007 I.C.J. 108, ¶¶ 209–10, 400 (Feb. 26) (discussing the implicitly proportionate connection between the degree of one country's offense and another country's response); U.K. v. Alb., 1949 I.C.J. ¶ 17 (Apr. 9) (noting that a "charge of such exceptional gravity against a State would require a degree of certainty").

141. TALLINN MANUAL 2.0, *supra* note 45, at 82.

142. *Id.*

143. Egan, *supra* note 88, at 5.

144. *Id.* at 7.

145. Michael Morell & Suzanne Kelly, *Fmr. CIA Director Michael Morell: "This Is the Political Equivalent of 9/11"*, CIPHER BRIEF (Dec. 11, 2016), https://www.thecipherbrief.com/article/exclusive/fmr-cia-acting-dir-michael-morell-political-equivalent-911-1091 [https://perma.cc/QK8K-5X2X].

infiltration, and if the response is not visible, the deterrent effect is lost.[146] Transparency objectives are inhibited in cyber-operations law in part because the domain itself is still relatively new and evolving. There are also complications in implementing a geographic- and location-based legal structure alongside an incongruous Internet. Additional obstacles include the inevitable need for secrecy in carrying out most cyber operations and the attribution work that must occur regarding the cyber activities of our adversaries. Still, States should work toward norms of expected conduct in cyberspace, along with mutually agreed deterrents to harmful cyber intrusions. Such norms could supplement customary law on State responsibility, becoming *lex specialis* in the cyber domain.[147]

International law as summarized in *Tallinn 2.0* requires much less proof of attribution than lawyers traditionally expect.[148] Of course lawyers expect rigorous standards for proof in civil trials or criminal prosecution, not necessarily in national security investigations, depending on the investigative method. The proof necessary for attribution in cyber exploitation involving State responsibility certainly need not stand up in court. Indeed, the evidence of attribution may never be made public because of the sensitivity of the intelligence sources and methods utilized in the investigation.

Nonetheless, the international-law reasonableness approach and the absence of burdens or criteria for assessing attribution leave an unfortunate gap in the international law of cyber. Without more public accounting of State responsibility, governments and citizens are not likely to trust or accept cyber responses, leading to the escalation of cyber conflict and failures of deterrence. In the United States and much of the world, neither governments nor citizens will accept cyber operations without some credible attribution that is transparent to some degree.

Conclusions

States are better able to attribute cyber intrusions than they were a decade ago, but the technical environment is so dynamic that new tools constantly both improve and occlude attribution capabilities. Even though the attribution bar at international law is low, spoofing and other challenges can greatly complicate attribution and cyber response when an immediate response is required, particularly when a State is the suspected perpetrator. Attribution is in any case an all-source enterprise. States that are forced by international law to publicly express the proof of attribution to explain countermeasures or some other response run the risk of overstating their case,

---

146. *Id.*

147. *See supra* text accompanying notes 109–12 (discussing how States could develop specialized rules for State responsibility for cyber acts).

148. *See* TALLINN MANUAL 2.0, *supra* note 45, at 81 (asserting that States "must act as reasonable States would" in dealing with attribution uncertainty).

or not supporting it thoroughly, and thereby engage in an internationally wrongful act.

As cyber international relations now stand, a few States (the United States and likely Russia, China, North Korea, and Iran) benefit from the absence of express cyber norms on what suffices to attribute State responsibility for cyber exploitation because they have the most offensive cyber capabilities. Russian State involvement in the DNC hacks and the releases through WikiLeaks is a good example. Because it is unclear whether the Russian interference in the U.S. elections amounted to the coercion that is necessary to establish an international law violation, the Putin government could and did act with relative impunity. Establishing attribution of the hacks and dissemination to WikiLeaks to the Russian government was a multifaceted intelligence investigation that could not be completed with confidence in short order. Countermeasures could not be lawfully implemented, and the late-arriving self-help retorsion measures likely did nothing to deter further Russian cyber aggression.

The decision to delay formal attribution of the DNC hacks to Russia was a policy decision. As noted above, President Obama had declined to name Russian State involvement in cyber intrusions because of fear of escalating to cyberwar, and because of the presumed need for Russian cooperation in Syria negotiations.[149] Situation Room meetings on the Russian hacking began in July 2016, but no formal attribution report was forwarded to the President.[150] During August, a series of formerly secretive software tools that can be used for cyber surveillance or attack were published by a hacking group possibly affiliated with Russia. U.S. officials took the dissemination of the tools as a warning that Russia would respond with more releases of U.S. secrets if the United States retaliated for the DNC hack.[151] Reportedly, a series of meetings around the same time deliberated aggressive cyber counterstrikes, although none of those recommendations were formally presented to the President.[152] Officials worried that an aggressive U.S. response would undermine confidence in our voting system, and perhaps most importantly, should not be seen as trying to influence the election.[153] Instead, President Obama delivered his personal warning to Mr. Putin at the Group of 20 summit meeting and left the public attribution of Russia's role to the written statement from ODNI and DHS.

The States that benefit presently from the absence of rules in cyberspace are also the most vulnerable to cyber intrusions. As the most advanced cyber States begin to recognize the zero-sum aspects of cyber escalation, those

149. Lipton et al., *supra* note 1.
150. *Id.*
151. *Id.*
152. *Id.*
153. *Id.*

States should become more transparent about attribution in service of the mutual restraint that could be gained by sharing attribution information.[154] Extensive diplomatic, intelligence, and public communication about attribution and potential uses of countermeasures in the below-threshold cyber domain will become part of emerging customary international law as lawyers and government officials engage in this especially important risk assessment project. States should strive to establish criteria or measures for State attribution in instances of cyber exploitation, then seek bilateral or multilateral agreements with other States, toward establishing more concrete customary international law for attribution. Similar steps could be taken to agree on measures of public transparency on State responsibility.

The lack of clear normative bases for governing cyber operations according to international law extends beyond problems of attribution, of course. The same inadequacy of lawful, defensive response options that reveal themselves in discussing attribution fare no better when responsibility for a cyber intrusion is known. For example, *Tallinn 2.0* regards State sovereignty as a binding rule of international law[155] that applies to the conduct of nonconsensual cyber operations of one State against cyber infrastructure located in another State. Under this admittedly widely held view of sovereignty, the Russian DNC hack probably violated sovereignty and thus international law. The fact that the United States responded with relatively nonthreatening self-help retorsion may indicate that the United States views the noncoercive hacks and exfiltration of data not as internationally wrongful acts, but instead as a species of espionage that is generally unregulated by international law.[156]

Given the architecture of the Internet, the traditional Westphalian stance on sovereignty embedded in customary law and reflected by the IGE in *Tallinn 2.0* may frustrate the development of workable norms for controlling below-threshold conflict in cyberspace.[157] Consider the simple example of a nonstate, transnational terrorist group spreading malware across several States. Although many States are equipped to disrupt botnets or malware impacts through straightforward, technical cyber operations, the sovereignty rule could stand in the way of State responses to the terrorists that cross national borders. Absent State consent, any cyber operation in response to

154. In the United States, domestic law authorizes covert action, including for cyber activities. 50 U.S.C. § 3093 (2012). The fact that a domestic law justification exists for secrecy does not impact existing or evolving international law.

155. TALLINN MANUAL 2.0, *supra* note 45, at 11.

156. Egan, *supra* note 88, at 11–12; TALLINN MANUAL 2.0, *supra* note 45, at 85.

157. The United States' view is that "remote cyber operations involving computers or other networked devices located on another State's territory do not constitute a *per se* violation of international law." Egan, *supra* note 88, at 11. The U.S. view takes into account the importance of intelligence collection abroad through cyber means. *Id.* at 11–12.

this kind of intrusion that constitutes a prohibited intervention is unlawful. The barrier applies to responses to States and to nonstate actors.[158]

Tallinn 2.0 marks an important but early point in a conversation among States about the most important principles of international law in cyber. The conversation matters a great deal because so much of our international relations are now bound up in the cyber domain, and the existing rules of the road are riddled with gray areas and incomplete understandings.

158. Colonel Gary Corn, *Tallinn Manual 2.0—Advancing the Conversation*, JUST SECURITY (Feb. 15, 2017), https://www.justsecurity.org/37812/tallinn-manual-2-0-advancing-conversation/ [https://perma.cc/7LF6-AJL7].

* * *

Give Them an Inch, They'll Take a Terabyte: How States May Interpret *Tallinn Manual 2.0*'s International Human Rights Law Chapter

Robert E. Barnsby and Shane R. Reeves*

> The development of norms for [S]tate 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 [S]tate behavior—in times of peace and conflict—also apply in cyberspace.[1]

Introduction

The recent publication of *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, the "follow-on initiative [expanding *Tallinn Manual 1.0*'s] scope to include the public international law governing cyber operations during peacetime,"[2] is a truly remarkable accomplishment in both cyber and international law. Unquestionably, it is the most comprehensive work ever written to describe how international law regulates cyber activities that take place below the use-of-force threshold. As this Article underscores, the significance of the *Manual*'s publication is further enhanced by its Chapter seeking to "articulate[] Rules indicating the scope of application and content of international human rights law [(IHRL)] bearing on cyber activities."[3]

---

* Robert E. Barnsby is an Assistant Professor of Law at West Point and the Army Cyber Institute's Cyber Law Fellow. Shane R. Reeves is an Associate Professor and Deputy Head of the Department of Law at West Point and a Lieutenant Colonel in the United States Army. The views expressed here are their personal views and do not necessarily reflect those of the Department of Defense, the United States Army, the United States Military Academy at West Point, or any other department or agency of the United States Government. The analysis presented here stems from their academic research of publicly available sources, not from protected operational information. This article refers throughout its text to States (capitalized when used in accordance with the Westphalian / International Humanitarian Law (IHL) nation-state concept), Internet (capitalized), and cyberspace (one word), all consistent with the *Tallinn Manual*'s usage of those same terms.

1. WHITE HOUSE, INTERNATIONAL STRATEGY FOR CYBERSPACE: PROSPERITY, SECURITY, AND OPENNESS IN A NETWORKED WORLD 9 (2011), https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf [https://perma.cc/49T9-QUER].

2. TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS 1 (Michael Schmitt & Liis Vihul eds., 2017) [hereinafter TALLINN MANUAL 2.0].

3. *Id.* at 179.

An international group of "scholars and practitioners with expertise in the legal regimes implicated by peacetime cyber activities"[4] (International Group of Experts) authored the *Manual* (*Tallinn 2.0*) between 2013 and 2016 over the course of a series of formal meetings and workshops held in Tallinn, Estonia.[5] Like the *Manual* itself, it is inevitable that the *Manual*'s IHRL Chapter will be studied and debated endlessly. Less concerned with this overall debate than with the need for practitioners to understand specific assertions made within the human rights Chapter, this Article closely examines certain key terms in the text to ascertain their impact on daily cyber activities at the State (national) level. A granular view of the IHRL Chapter reveals these key terms to be often vague and ill-defined, resulting in definitional gaps capable of being used by States to undermine IHRL progress over time.

After background discussion laying the foundation for IHRL and identifying the actual human rights contemplated by the International Group of Experts in the IHRL Chapter (Part II), this Article identifies several important yet undefined terms and concepts throughout the work. Part III centers on perhaps the most significant example of an undefined concept, "countering terrorism,"[6] which the Experts state without further explanation to be a "legitimate purpose" allowing States to monitor online communications without violating the right to privacy.[7] While the International Group of Experts offers checks on possible abuse, this section demonstrates the challenges of constraining a State intent on using the "countering terrorism" exception to swallow the rule requiring States to respect and protect international human rights.[8] Even key terms such as the word "terrorism" are nebulous to the reader and exemplify the ambiguity on which a State may rely to limit human rights.[9]

---

4. *Id.* at 1.

5. *Id.* at 5–6. Tallinn, Estonia has embraced its status as home to NATO's Cooperative Cyber Defence Centre of Excellence (NATO CCD COE), "a renowned research and training institution," *id.* at 1, virtually ever since "Estonia suffered massive cyber attacks, primarily from ethnic Russian non-state actors" in 2007. Michael N. Schmitt, *The Law of Cyber Warfare:* Quo Vadis*?*, 25 STAN. L. & POL'Y REV. 269, 269 (2014).

6. TALLINN MANUAL 2.0, *supra* note 2, at 203.

7. *Id.*

8. The International Group of Experts identifies five rules that form the basis of IHRL's bearing on cyber activities. Rule 34 states that IHRL is "applicable to cyber-related activities." *Id.* at 182. Rule 35 states that "[i]ndividuals enjoy the same international human rights with respect to cyber-related activities that they otherwise enjoy." *Id.* at 187. Rule 36 outlines "[o]bligations to respect and protect international human rights," as further elucidated throughout the text of this Article. *Id.* at 196. Rule 37 reminds the reader that "[t]he obligations to respect and protect international human rights . . . remain subject to certain limitations that are necessary to achieve a legitimate purpose," as discussed throughout this Article. *Id.* at 201–02. Rule 38 contemplates "[a State's ability to] derogate from its human rights treaty obligations . . . when permitted, and under the conditions established, by the treaty in question." *Id.* at 207.

9. *See infra* notes 37–45 and accompanying text.

Part IV analogizes the gaps in *2.0* to a similarly critical, unforeseen gap in *Tallinn 1.0* (above the use-of-force-threshold activities) to illustrate how both manuals similarly act as a general framework for application of international law to cyber activities while leaving specifics to be filled in by State practice. Although the International Group of Experts is not optimistic there will be more than a paucity of State practice[10] available due to secrecy challenges, and provides another vague term suggesting "effective measures"[11] will be allowed, this Article suggests there are examples of unclassified, ongoing State practices that both help define the vague "effective measures" term and indicate the ability to overcome the secrecy challenge in this area. Unclassified U.S. cyber programs designed to gather intelligence, map networks, and prepare for military operations against an adversary in the cyber realm are described here in an effort to illustrate the (perhaps) overstated secrecy concerns.[12] Finally, mindful that "[m]any commentators assert customary international law as they would like it to be, rather than as it actually is,"[13] this Article does not suggest any particular State practice has risen to the level of customary international law in these areas. Nevertheless, the aspects of State practice described *infra* amplify our understanding of what the IHRL Chapter seeks to achieve with its admirable efforts to codify online rights "in accordance with international human rights law."[14]

I. Background

The United Nations Charter lays the foundation for international human rights law. While primarily a *jus ad bellum* instrument, the purposes and principles of the charter recognize the need for human rights and "for fundamental freedoms for all without distinction as to race, sex, language, or religion."[15] This statement ensures the protection of persons as individuals "rather than as subjects of sovereign States" and imposes certain legal requirements on State actors.[16] Composed of both treaty[17] and customary

10. *See infra* note 74 and accompanying text.

11. TALLINN MANUAL 2.0, *supra* note 2, at 199.

12. *See infra* notes 85–87 and accompanying text.

13. John B. Bellinger, Legal Advisor, U.S. Dep't of State, Lecture by Mr. Bellinger for Oxford Leverhulme Programme on the Changing Character of War (Dec. 10, 2007), https://2001-2009.state.gove/s/l/2007/112723.htm [https://perma.cc/V9PJ-XCNC].

14. TALLINN MANUAL 2.0, *supra* note 2, at 179.

15. U.N. Charter art. 1, ¶ 3; *see also* Brian J. Bill, *Human Rights: Time for Greater Judge Advocate Understanding*, ARMY LAW., June 2010, at 54, 54–55 (discussing cursorily the United States' role in the development of international human rights law).

16. RICHARD P. DIMEGLIO ET AL., U.S. ARMY JUDGE ADVOCATE GEN.'S LEGAL CTR. & SCH., INT'L & OPERATIONAL LAW DEP'T, LAW OF ARMED CONFLICT DESKBOOK 195 (William J. Johnson & Andrew D. Gillman eds., 2012) [hereinafter DESKBOOK].

17. *See, e.g.*, International Covenant on Civil and Political Rights, Dec. 16, 1966, 999 U.N.T.S. 171 (committing its State signatories to protection of the civil and political rights of individuals).

obligations, this body of international law, as noted throughout the *Tallinn Manual 2.0* IHRL Chapter, applies in cyberspace.[18]

While no definitive list of human rights in cyberspace exists,[19] certain rights are especially relevant in the cyber context. The International Group of Experts provides a nonexhaustive list of particularly important human rights applicable in cyberspace, including freedom of expression, freedom of opinion, due process, and perhaps most importantly, privacy.[20] Rule 35 of the IHRL Chapter notes the central importance of privacy in cyberspace but also cautions that the precise scope of the right is unsettled.[21] Further, the International Group of Experts acknowledges the view that the right to privacy has "not yet crystallized into a customary norm."[22] Yet, despite these caveats, a reading of the *Manual* makes clear that an individual's right to privacy in cyberspace, similar to other international human rights,[23] is to be respected and protected by State actors.[24]

Furthermore, although certain fundamental human rights are considered nonderogable,[25] such as the prohibition on slavery, the prohibition on torture, and the right to recognition as a person before the law,[26] the International

---

18. Specifically, Rule 34 states that "[i]nternational human rights law is applicable to cyber-related activities." TALLINN MANUAL 2.0, *supra* note 2, at 182. Rule 35 states that "[i]ndividuals enjoy the same international human rights with respect to cyber-related activities that they otherwise enjoy." *Id.* at 187. The International Group of Experts "agreed that both treaty and customary international human rights law apply to cyber-related activities, [though] they cautioned that it is often unclear as to whether certain human rights reflected in treaty law have crystallised as rules of customary law." *Id.* at 179. Making clear that "States may, under specific circumstances . . . , limit the exercise and enjoyment of certain rights," *id.*, this entire Chapter in *Tallinn 2.0* is reflective of the ability to limit States' "obligations to respect and protect international human rights." *Id.* at 201 (Rule 37). While ostensibly necessary to circumscribe nonabsolute (or fundamental) rights, the Group of Experts' empowerment of States' abilities to define for themselves what is "necessary to achieve a legitimate purpose," *id.* at 202 (Rule 37), is significant, as described throughout Part III.

19. *See, e.g.*, Bill, *supra* note 15, at 59 (noting that the international community is consistently expanding human rights law).

20. TALLINN MANUAL 2.0, *supra* note 2, at 187 (Rule 35).

21. *Id.* at 189.

22. *Id.*

23. International human rights laws are designed "to induce states to remedy the inadequacies of their national laws and institutions," thus ensuring these individual protections are "respected and vindicated." Louis Henkin, *Introduction* to THE INTERNATIONAL BILL OF RIGHTS: THE COVENANT ON CIVIL AND POLITICAL RIGHTS 14 (Louis Henkin ed., 1981).

24. *See* TALLINN MANUAL 2.0, *supra* note 2, at 196 (Rule 36) (requiring State actors to respect and protect international human rights).

25. "Derogation refers to the legal right to suspend certain human rights treaty provisions in time of war or in cases of national emergencies. Certain fundamental (customary law) rights, however, may not be derogated from . . . ." DESKBOOK, *supra* note 16, at 205 (emphasis omitted).

26. *See* G.A. Res. 217 (III) A, Universal Declaration of Human Rights (Dec. 10, 1948) (listing human rights to which all people are entitled and denying recognition of any State right to "engage in any activity or to perform any act aimed at the destruction of any of the rights and freedoms set forth herein"). For a discussion on whether the Universal Declaration has ripened into customary international law, see Hurst Hannum, *The Status of the Universal Declaration of Human Rights in National and International Law*, 25 GA. J. INT'L & COMP. L. 287, 317–52 (1996). The same

Group of Experts notes that privacy "is not an absolute right and may be subject to limitations, as discussed in Rule 37."[27] Thus, Rule 37—"[t]he obligations to respect and protect international human rights, with the exception of absolute rights, remain subject to certain limitations that are necessary to achieve a legitimate purpose, nondiscriminatory, and authorized by law"—offers a methodology for limiting the international human right of privacy in cyberspace.[28]

As a final background matter for purposes of this Article, the International Group of Experts outlines the effect of secrecy as a barrier to understanding State practice in cyberspace, arguing that "State cyber practice is mostly classified and publicly available expressions of *opinio juris* are sparse, [making it] difficult to definitively identify any cyber-specific customary international law."[29] While this statement accurately captures aspects of the contemporary environment, specific State practice in cyberspace is increasingly available to the public[30] and, in time, can ripen into customary international law. Though not yet at the level of customary international law, certain State practice in cyberspace, and a discussion of its relevance, are key subjects to which this Article returns below.

II. Is Countering Terrorism a Legitimate Reason to Violate the Right to Privacy in Cyberspace?

Importantly, Rule 37 of the IHRL Chapter states that the "obligations to respect and protect international human rights, with the exception of absolute

---

prohibition on derogation applies in the cyber context. TALLINN MANUAL 2.0, *supra* note 2, at 208. However, the *Manual* differentiates between the impermissibility of limiting a human right and the notion of nonderogability. *Id.* at 202–03.

27. TALLINN MANUAL 2.0, *supra* note 2, at 189.

28. *Id.* at 201–02. Cyberspace is defined as "a global domain within the information environment that encompasses the interdependent networks of information technology infrastructures, including the Internet and telecommunication networks." U.S. DEP'T OF DEF., QUADRENNIAL DEFENSE REVIEW REPORT 37 (2010) [hereinafter DEFENSE REVIEW REPORT]. *Tallinn Manual 1.0* defines cyberspace as "[t]he environment formed by physical and non-physical components, characterized by the use of computers and the electro-magnetic spectrum, to store, modify, and exchange data using computer networks." TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE 258 (Michael Schmitt ed., 2013) [hereinafter TALLINN MANUAL 1.0].

29. TALLINN MANUAL 2.0, *supra* note 2, at 3.

30. Some States share this information by choice. *See, e.g.*, JOINT CHIEFS OF STAFF, JOINT PUBLICATION 3-12(R): CYBERSPACE OPERATIONS (2013) [hereinafter JOINT PUBLICATION 3-12(R)], http://www.dtic/mil/doctrine/new_pubs/jp3_12R.pdf [https://perma.cc/RH4E-DHTA] (describing the United States' military operations in and through cyberspace in an unclassified document easily accessible over the Internet). In other instances, States' cyber activities are being exposed. *See, e.g.*, Daniel Garrie & Shane R. Reeves, *An Unsatisfactory State of the Law: The Limited Options for a Corporation Dealing with Cyber Hostilities by State Actors*, 37 CARDOZO L. REV. 1827, 1829–30, 1835–36 (2016) (discussing a number of unattributed cyber acts conducted by State actors); Frank Langfitt, *U.S. Security Company Tracks Hacking to Chinese Army Unit*, NPR (Feb. 19, 2013), http://www.npr.org/2013/02/19/172373133/report-links-cyber-attacks-on-u-s-to-chinas-military [https://perma.cc/L87Z-RJ9M].

rights, remain subject to certain limitations."[31] Recognizing the sensitivity of placing limitations on international human rights, Rule 37's commentary expounds on the limitation criteria and their applicability.[32] While the International Group of Experts discusses the need to ground any limitation in international law[33] and for these measures to be nondiscriminatory,[34] the greatest ambiguity in the applicability of Rule 37 surrounds the meaning of "legitimate purpose." In an effort to establish parameters for whether a limitation serves a legitimate purpose, the International Group of Experts offers in the commentary a nonexhaustive list of legitimate purposes, including: "protection of rights and reputations of others, national security, public order, public health, [and] morals."[35] To provide even a greater understanding of the term, the commentary gives an example: "For instance, countering terrorism is a legitimate purpose that allows States to monitor particular online communications without thereby violating the right to privacy."[36]

Despite the admirable attempt of the International Group of Experts to define a "legitimate purpose," the term remains overly broad. The commentary's countering-terrorism example most starkly illustrates this point. Currently, there is no universally accepted definition of "terrorism,"[37] and the parameters of the term remain contentiously debated.[38] As a result,

---

31. TALLINN MANUAL 2.0, *supra* note 2, at 201–02.

32. *Id.* at 202–03.

33. *See id.* at 202 ("[T]he basis for a limitation on the enjoyment or exercise of an international human right must be provided for in international law.").

34. *See id.* at 206 ("Restrictions on cyber activities that are otherwise protected by international human rights law must be non-discriminatory.").

35. *Id.* at 203.

36. *Id.*

37. Since 1996, an effort within the United Nations has been ongoing to develop the Comprehensive Convention on International Terrorism. G.A. Res. 51/210, ¶ 9 (Dec. 17, 1996) (establishing an ad hoc committee to develop "a comprehensive legal framework of conventions dealing with international terrorism"). However, the negotiations are consistently deadlocked due to disagreements over the definition of the term. *See Ad Hoc Committee Established by General Assembly Resolution 51/210 of 17 December 1996*, UNITED NATIONS OFF. LEGAL AFFAIRS, http://legal.un.org/committees/terrorism/ [https://perma.cc/S5JU-CCMD] (outlining the ongoing emphasis on developing the treaty in order to eliminate international terrorism); Press Release, General Assembly, Legal Committee Urges Conclusion of Draft Comprehensive Convention on International Terrorism, U.N. Press Release GA/L/3433 (Oct. 8, 2012) (urging an agreement on a clear definition of "terrorism").

38. *See* ANGUS MARTYN, AUSTL. DEP'T PARLIAMENTARY LIBRARY, THE RIGHT OF SELF-DEFENCE UNDER INTERNATIONAL LAW—THE RESPONSE TO THE TERRORIST ATTACKS OF 11 SEPTEMBER 3 (2002), http://www.aph.gov/au/binaries/library/pubs/civ/2001-02/02cib08.pdf [https://perma.cc/DSR3-7ADK] ("The international community has never succeeded in developing an accepted comprehensive definition of terrorism."); James Hess, *The Challenge of Defining Terrorism Around the World*, IN PUBLIC SAFETY (July 13, 2015), http://inpublicsafety.com/2015/07/the-challenge-of-defining-terrorism-around-the-world/ [https://perma.cc/XG8R-U3AV] ("Those familiar with the study of terrorism know there is not a universally accepted definition.").

there is a myriad of national and regional definitions for "terrorism."[39] The closest the international community has come to an understanding of the concept is in United Nations Security Council Resolution 1566, which forbids:

> criminal acts, including against civilians, committed with the intent to cause death or serious bodily injury, or taking of hostages, with the purpose to provoke a state of terror in the general public or in a group of persons or particular persons, intimidate a population or compel a government or an international organization to do or to abstain from doing any act . . . .[40]

The resolution, however, is unhelpful as it is nonbinding and lacks authority in international law.[41] Further, its offered definition of "terrorism" is sufficiently vague to allow for individual State interpretations. "Terrorism," therefore, can encompass a wide range of activities and, in its nebulous conception, is highly susceptible to States' infringement on individuals' right of privacy in cyberspace.

Similarly, the broad concept of "countering terrorism" is too expansive to be a "legitimate purpose." "Counterterrorism," like "counterinsurgency,"[42] is a far-reaching strategic term that is expansively applied to a variety of circumstances. Described by the United States as "activities and operations . . . taken to neutralize terrorists, their organizations, and networks in order to render them incapable of using violence to instill fear and coerce governments or societies to achieve their goals," the concept is intentionally broad to allow for a variety of responses.[43] Countering terrorism, in other words, is whatever a State does to "disrupt, isolate, and dismantle terrorist organizations."[44] Admittedly, States are obligated to comply with international human rights law when implementing

---

39. Alex P. Schmid, *The Revised Academic Consensus Definition of Terrorism*, 6 PERSP. ON TERRORISM 158, 158 (2012), http://www.terrorismanalysts.com/pt/index/php/pot/article/view/schmid-terrorism-definition/385 [https://perma.cc/HTV7-LURW].

40. S.C. Res. 1566, ¶ 3 (Oct. 8, 2004).

41. Schmid, *supra* note 39, at 158.

42. Counterinsurgency (COIN) is described by the United States as "a comprehensive civilian and military effort designed to simultaneously defeat and contain insurgency and address its root causes. COIN is primarily a political struggle and incorporates a wide range of activities by the [host-nation] government of which security is only one, albeit an important one." JOINT CHIEFS OF STAFF, JOINT PUBLICATION 3-24: COUNTERINSURGENCY I-2 (2013) [hereinafter JOINT PUBLICATION 3-24], www.dtic.mil/doctrine/new_pubs/jp3_24.pdf [https://perma.cc/MDY5-3D7P].

43. *See* JOINT CHIEFS OF STAFF, JOINT PUBLICATION 3-26: COUNTERTERRORISM I-5 (2014) [hereinafter JOINT PUBLICATION 3-26], www.dtic.mil/doctrine/new_pubs/jp3_26.pdf [https://perma.cc/C5XD-Q5CL] (providing guidance to U.S. armed services for counterterrorism activities).

44. *Id.* at I-6.

their counterterrorism measures.[45] However, this obligation lacks specificity and allows wide latitude to States in determining how to "counter terrorism," including, if necessary, monitoring online personal communications.

Declaring that "countering terrorism" is a "legitimate purpose" for infringing upon the right to privacy in cyberspace is both vague and problematic. Equally troubling is the use of other broad and amorphous terms such as "national security," "public order," or "public health" to describe a "legitimate purpose."[46] By leaving the description of a "legitimate purpose" vague, Rule 37 gives State actors discretion, increasing the risk of overzealous limitations on international human rights in the cyber context. To its credit, the International Group of Experts does not ignore this problem and addresses this concern by emphasizing in the commentary that "[a] restriction on cyber activities that might otherwise be protected by international human rights law must be 'necessary.'"[47] However, this language is of questionable impact as the commentary immediately follows with the statement "although States enjoy a margin of appreciation in this regard."[48]

The International Group of Experts also raises the principle of proportionality, as it applies to limiting international human rights, as a check on overuse of Rule 37.[49] The idea of proportionality is extensively used throughout international law;[50] thus, it is helpful for the commentary to note expressly "that the need for any State interference with human rights in order to meet a legitimate State objective be assessed against the severity of the infringement on human rights."[51] The commentary goes on to state that the restriction must be the least intrusive means available to achieve the stated objective.[52] While disagreeing as to whether the proportionality principle is

45. *See* S.C. Res. 1624, ¶ 4 (Sept. 14, 2005) (requiring that States "comply with all of their obligations under international law, in particular international human rights law, refugee law, and humanitarian law" when conducting counterterrorism operations); *Terrorism/Counterterrorism*, HUMAN RIGHTS WATCH, https://www.hrw.org/topic/terrorism-counterterrorism [https://perma.cc/4SST-N6UB] ("Governments have a responsibility to protect those within their jurisdiction from extremist attacks, but must ensure that all counterterrorism measures respect human rights.").

46. TALLINN MANUAL 2.0, *supra* note 2, at 203.

47. *Id.*

48. *Id.*

49. *Id.* at 204–05.

50. For example, proportionality is one of the principles of the law of armed conflict. *See* Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflict (Protocol I) art. 51(5)(b), June 8, 1977, 1125 U.N.T.S. 3 [hereinafter AP I] (noting that proportionality determines whether "an attack . . . may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof [that would] be excessive in relation to the concrete and direct military advantage anticipated").

51. TALLINN MANUAL 2.0, *supra* note 2, at 204.

52. *Id.*

customary, the Experts note in the commentary that a majority "accepted a condition of proportionality."[53] In so doing, they agreed that "necessity alone does not suffice to justify limiting obligations" as it would be "incongruent with the object and purpose of limitations on international human rights law to permit a restriction that is necessary, but disproportionate to the State's interest in question."[54] Yet, again, after outlining this seeming restraint, the commentary goes on to note that State actors "enjoy a margin of appreciation" when applying the least-restrictive-means proportionality requirement.[55]

Rule 37 and its commentary consistently defer to States. This deference allows the State to determine unilaterally whether a limitation on an international human right in cyberspace is necessary to achieve a legitimate purpose and, if so, how to effectuate any limitations in a proportional manner. The vague and broad terminology used to describe a "legitimate purpose" further empowers the State to limit human rights in the cyber context if it so chooses. The Experts' use of generalities, including but not limited to the term "countering terrorism," and the deference shown to States throughout Rule 37, therefore leaves open the question of what exactly restrains a State from limiting international human rights in cyberspace.

III. Do Not Worry . . . State Practice Will Begin to Fill the Gaps

The uncertainty in Rule 37 is not surprising, as a granular analysis of such an ambitious and unprecedented project as the *Manual* will invariably reveal some gaps. This is similar to *Tallinn 1.0*,[56] which, in its attempt "to explain how the existing law of armed conflict generally regulate[d] cyber warfare," left certain specifics unaddressed.[57] For example, *Tallinn 1.0*'s Rule 27 states that "[i]n an international armed conflict, inhabitants of unoccupied territory who engage in cyber operations as part of a *levée en masse* enjoy combatant immunity and prisoner of war status."[58] Yet this

53. *Id.* at 205.

54. *Id.*

55. *Id.*

56. The *Tallinn Manual on the International Law Applicable to Cyber Warfare* was drafted to help governments "deal with the international legal implications of cyber operations." David Wallace & Shane R. Reeves, *The Law of Armed Conflict's "Wicked" Problem:* Levée en Masse *in Cyber Warfare*, 89 INT'L L. STUD. 646, 648 (2013); *see also* Jeremy Kirk, *Manual Examines How International Law Applies to Cyberspace*, IT WORLD (Sept. 3, 2012), http://www.itworld.com/article/2720628/it-management/manual-examines-how-international-law-applies-to-cyberwarfare.html [https://perma.cc/P8E6-JB7L] (reporting that the original *Tallinn Manual* was created by The Cooperative Cyber Defense Center of Excellence, which "assists NATO with technical and legal issues associated with cyberwarfare-related issues" in order to address a variety of cyber legal issues).

57. *See* Wallace & Reeves, *supra* note 56, at 648–49 (arguing that *Tallinn 1.0*'s application of the existing law of armed conflict to cyber warfare was too general to adequately address the problems of cyber warfare).

58. TALLINN MANUAL 1.0, *supra* note 28, at 102.

attempt "to reconcile the [traditional] concept of *levée en masse*[59] with the 'cyber conflicts between nations and ad hoc assemblages'" is simply impractical.[60] While there are a number of problems with the idea of a cyber *levée en masse*,[61] the most obvious is the traditional criteria that those participating in a spontaneous uprising carry arms openly.[62] The requirement to "carry[] arms openly" is of utmost importance in a *levée en masse* as these movements are done in emergency circumstances, leaving no time for organization or for participants to use distinctive signs.[63] With no other form of recognition, carrying a weapon becomes the "only distinguishing characteristic between a protected civilian and a combatant, and, therefore, who can be lawfully attacked."[64] Further, there is no question as to what "carrying arms openly" means for those participating in a *levée en masse*. The referred-to arms are clearly traditional weapons like rifles, hand grenades, and pistols.[65]

"Recognizing both the realities of a *levée en masse* and the criticality of protecting civilians, the law of armed conflict [thus] places singular emphasis on the essential need for those choosing to participate in a spontaneous uprising" to openly carry these conventional armaments.[66] Yet, in a cyber *levée en masse* the "weapon" used is a computer. While it is possible for a computer to be considered a "weapon,"[67] simple possession "cannot be

---

59. A *levée en masse* occurs when inhabitants of a nonoccupied territory, without time to form into a regular armed unit, spontaneously take up arms to resist an invading force. Those that take up arms forfeit their civilian status and become combatants. *See* Geneva Convention Relative to the Treatment of Prisoners of War art. 4(A)(6), Aug. 12, 1949, 6 U.S.T. 3316; GARY D. SOLIS, THE LAW OF ARMED CONFLICT: INTERNATIONAL HUMANITARIAN LAW IN WAR 200–01 (2010) (quoting the definition of *levée en masse* as stated in Prosecutor v. Delalić, Case No. IT-96-21-T, Judgment, ¶ 268 (Int'l Crim. Trib. for the Former Yugoslavia Nov. 16, 1998)). The idea behind a *levée en masse* is simple: during an invasion, the civilian population of unoccupied territory can spontaneously take up arms against the invading army to stop an occupation. YORAM DINSTEIN, THE CONDUCT OF HOSTILITIES UNDER THE LAW OF INTERNATIONAL ARMED CONFLICT 42 (1st ed. 2004).

60. *See* Wallace & Reeves, *supra* note 56, at 649 (quoting Stephen W. Korns & Joshua E. Kastenberg, *Georgia's Cyber Left Hook*, PARAMETERS, Winter 2008–09, at 60, 70).

61. *See id.* at 658–60 (discussing how the traditional occupied–unoccupied paradigm and mass-uprising aspects of a *levée en masse* are less relevant in the cyber context).

62. A *levée en masse* is expected to be a spontaneous uprising where inhabitants impulsively organize and are only distinguished as combatants by the open and visible carrying of arms. *See* COMMENTARY, III GENEVA CONVENTION RELATIVE TO THE TREATMENT OF PRISONERS OF WAR 67 (Jean S. Pictet ed., 1960) [hereinafter COMMENTARY, GC III] (explaining that the requirement of open carry is intended to protect the "combatants themselves who must be recognizable in order to qualify for treatment as prisoners of war").

63. Wallace & Reeves, *supra* note 56, at 657.

64. *Id.*

65. *See* COMMENTARY, GC III, *supra* note 62, at 61 (discussing the requirement of carrying arms openly, referring to weapons such as hand grenades or revolvers).

66. Wallace & Reeves, *supra* note 56, at 657.

67. *Tallinn 1.0* defines a cyber weapon as "cyber means of warfare that are by design, use, or intended use capable of causing either (i) injury to, or death of, persons; or (ii) damage to, or

interpreted to be indicative of combatant activity."[68] The *Tallinn 1.0* International Group of Experts recognized this reality by noting, "even if [computers] qualify as weapons, the requirement to carry arms openly has little application in the cyber context."[69] A detailed law of armed conflict (LOAC) analysis reveals key challenges related to this area: namely, the impossibility of distinguishing participants in a cyber *levée en masse* and, subsequently, the inability of participating individuals to comply with the required LOAC principle of distinction.[70]

The *Tallinn 1.0* International Group of Experts understood the difficulties with the concept of a cyber *levée en masse* and even "highlight[ed] various unanswered and troubling questions in the commentary to Rule 27."[71] The Experts were also aware that a general application of the existing LOAC to cyber warfare does not always work[72] and future legal developments are necessary to address the nuanced issues generated by the novelties of cyber warfare.[73] Yet, due to "the relative infancy of cyber operations and paucity of state practice,"[74] the *Tallinn 1.0* International Group of Experts only addressed the "law currently governing cyber conflict."[75] Avoiding theoretical debates,[76] *Tallinn 1.0* thus provided a general regulatory framework capable of allowing the LOAC to evolve, as

---

destruction of, objects, that is, causing the consequences required for qualification of a cyber operation as an attack." TALLINN MANUAL 1.0, *supra* note 28, at 141–42.

68. Wallace & Reeves, *supra* note 56, at 659.

69. TALLINN MANUAL 1.0, *supra* note 28, at 100.

70. The principle of distinction states that "[i]n order to ensure respect for and protection of the civilian population and civilian objects, the Parties to the conflict shall at all times distinguish between the civilian population and combatants and between civilian objects and military objectives." AP I, *supra* note 50, art. 48. For additional discussions on applying the principle of distinction in cyberspace, see Robin Geib & Henning Lahmann, *Cyber Warfare: Applying the Principle of Distinction in an Interconnected Space*, 45 ISR. L. REV. 381, 384 (2012) (theorizing that nonmilitary components of cyberspace itself will become targets of cyberwarfare operations); Noam Lubell, *Lawful Targets in Cyber Operations: Does the Principle of Distinction Apply?*, 89 INT'L L. STUD. 252, 264 (2013) (recognizing complicated questions surrounding the threshold level of harm required for cyber operations to become "attacks" subject to the LOAC).

71. Wallace & Reeves, *supra* note 56, at 658–59; *see also* TALLINN MANUAL 1.0, *supra* note 28, at 102–03 (discussing various problems with the concept of a cyber *levée en masse* and the limited circumstances in which it would apply).

72. *See* Wallace & Reeves, *supra* note 56, at 649 (noting that a cyber *levée en masse* "illustrates how ill-suited, and often impractical, the existing law of armed conflict can be when applied in the cyber context").

73. TALLINN MANUAL 1.0, *supra* note 28, at 5 (noting that the *Manual* does not cover best practices or preferred policies); *see also* Schmitt, *supra* note 5, at 274 (noting that for States to be successful in cyberspace they will need to depart from "the received norms that have been set forth by the International Group of Experts in the *Tallinn Manual*").

74. Schmitt, *supra* note 5, at 270.

75. TALLINN MANUAL 1.0, *supra* note 28, at 5.

76. The 95 "Black Letter Rules" of *Tallinn 1.0* still "sometimes evoked ardent and nuanced debate," with the "commentary accompanying each Rule captur[ing] these debates and highlight[ing] those which remain unresolved." Schmitt, *supra* note 5, at 271.

necessary, to address the unanticipated complexities that emerge in cyberspace.[77]

Similar to *Tallinn 1.0*, *Tallinn 2.0*'s IHRL Chapter acts as a broad foundational document that intentionally leaves room for further legal developments. As noted in Part III, the International Group of Experts occasionally refers to terms without adding specificity to their meaning. For example, the commentary to Rule 36 states:

> The Internet has been used for terrorist purposes, such as recruitment for, incitement of, and the financing of terrorism. The International Group of Experts agreed that "States have both a right and a duty to take effective measures to counter the destructive impact of terrorism on human rights," even though some measures taken by the State may affect human rights such as the freedom of expression and the right of privacy. Any such measures must comply with Rule 37.[78]

Like the term "legitimate purpose" in the commentary to Rule 37, the Rule 36 language leaves open a critical question—namely, what constitutes "effective measures" States have a right and duty to undertake in this context? Moreover, what is an effective measure that rises to the level of a legitimate purpose for limiting the international human right of privacy in the cyber context?[79]

The United States has begun to answer this question by publicly advertising the measures it employs to "counter terrorism" in cyberspace. The United States requires "[i]nformation-related capabilities such as . . . cyberspace operations . . . [to] be applied to [counterterrorism] operations as a means to influence extremists, their supporters, and the mainstream populace."[80] These cyber operations, nested within the United States' counterterrorism efforts, are "composed of the military, intelligence, and ordinary business operations of [the Department of Defense] in and through cyberspace."[81]

While this broad definition of cyberspace operations may not be tremendously helpful, Joint Publication 3-12(R), an unclassified military document titled "Cyberspace Operations," provides some clarity. The document notes that "successful execution of [cyberspace operations] requires the integrated and synchronized employment of offensive, defensive, and DODIN operations, underpinned by effective and timely

---

77. *See, e.g.*, DEFENSE REVIEW REPORT, *supra* note 28, at 62 (noting that rising complexities in cyberspace "pose new security challenges that require innovative adjustments to our defense posture").

78. TALLINN MANUAL 2.0, *supra* note 2, at 199.

79. *See supra* notes 34–36 and accompanying text (discussing the nature of a "legitimate purpose" as a justification for restricting international rights).

80. JOINT PUBLICATION 3-26, *supra* note 43, at V-6.

81. JOINT PUBLICATION 3-12(R), *supra* note 30, at vii.

operational preparation of the environment [(OPE)]."[82] It goes on to state that categorization of a cyberspace operation is dependent upon the intent behind the mission.[83] However, "these missions . . . require the employment of various capabilities to create specific effects," and therefore the document discusses a number of particular actions in cyberspace.[84]

In so doing, it becomes possible to determine what type of cyber activities are considered part of "cyberspace operations" and subsequently are included as cyberspace measures in United States counterterrorism operations. Cyberspace Intelligence, Surveillance, and Reconnaissance (C-ISR), which gathers intelligence to support a future offensive or defensive cyber operation[85] and maps adversary cyberspace to support military planning,[86] is one example of a listed activity. Additionally, cyberspace operational preparation of the environment (C-OPE), which "consists of the non-intelligence enabling activities conducted to plan and prepare for potential follow-on military operations,"[87] is also a described cyber action.

Some of the described actions, such as "cyberspace attack,"[88] clearly cross the use-of-force threshold and would not be regulated by the international law contemplated in *Tallinn 2.0*.[89] However, C-ISR and C-OPE

---

82. *Id.* Offensive cyber operations (OCO) are "intended to project power by the application of force in and through cyberspace." *Id.* Defensive cyber operations (DCO) are "intended to defend DOD or other friendly cyberspace." *Id.* The Department of Defense Information Network (DoDIN) "is a global infrastructure of Department of Defense (DOD) systems carrying DOD, national security, and related intelligence community information and intelligence." *Id.* at vi.

83. *Id.* at vii.

84. *Id.* at II-4 to -5.

85. *Id.*

86. *Id.* C-ISR "requires appropriate deconfliction, and cyberspace forces that are trained and certified to a common standard with the [intelligence community]. ISR in cyberspace is conducted pursuant to military authorities and must be coordinated and deconflicted with other [United States Government] departments and agencies." *Id.*

87. *Id.* at II-5. Operational preparation of the environment is defined as "[t]he conduct of activities in likely or potential areas of operations to prepare and shape the operational environment." JOINT CHIEFS OF STAFF, JOINT PUBLICATION 3-05: SPECIAL OPERATIONS GL-9 (2014), www.dtic.mil/doctrine/new_pubs/jp3_05.pdf [https://perma.cc/3SMP-SFYN].

88. Cyberspace attack is defined 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." JOINT PUBLICATION 3-12(R), *supra* note 30, at II-5. *Deny*, *degrade*, and *disrupt* are all defined. *See id.*

89. Of course, these activities must fall below the use-of-force threshold for *Tallinn 2.0* to apply. "[S]tates and scholars have struggled mightily to define the threshold at which an act becomes a 'use of force.'" Schmitt, *supra* note 5, at 279. While there is no bright-line test that determines if a cyber operation is a use of force, there are a number of factors that inform this determination. *See id.* at 280 (enumerating these factors). The *Tallinn 1.0* International Group of Experts created a nonexhaustive list that includes:

> severity, immediacy, directness, invasiveness, measurability, military character, state involvement, and presumptive legality. Additional factors found meaningful by the Experts included, inter alia, the prevailing political environment, the nexus of an operation to prospective military force, the attacker's identity, the attacker's track record with respect to cyber operations, and the nature of the target. These and other

most likely fall below the use-of-force line as, by definition, they do not cause damage, injury, or even severe nonphysical consequences.[90] Instead, these cyber activities focus on intelligence gathering and planning for future military operations, both of which are peacetime activities. As a result, it becomes possible to start determining what cyber measures below the use of force the United States employs to counter terrorism.

Understanding what cyber activities below the use-of-force threshold the United States employs in its counterterrorism efforts thus helps to define the term "effective measure" as undertaken in the Rule 36 context. More importantly, it evinces State practice and begins to represent the legal developments necessary to fill in the gaps left open by *Tallinn 2.0*'s IHRL Chapter. Of course, the United States' practice is a singular example of one nation's behavior and is clearly not a customary norm. Yet it is an important representation of how State practice can provide the specificity currently missing in *Tallinn 2.0* while simultaneously illustrating how the international law regulating cyber operations is likely to develop in the future.

IV. Conclusion

Similar to *Tallinn 1.0*, *Tallinn 2.0* is an unprecedented attempt to codify international law, albeit below the use-of-force threshold, in cyber operations.[91] It is an objective restatement of the *lex lata*, versus a reflection of *lex ferenda*,[92] for the same reason *Tallinn 1.0* only analyzed current international law: namely, to avoid making questionable predictions about how the law should develop.[93] Instead, the International Group of Experts behind *Tallinn 2.0*, and specifically its International Human Rights Law

---

> factors operate in concert as [S]tates make case-by-case determinations. Of them, only severity alone can qualify a cyber operation as a use of force.

Id. at 280–81 (citing TALLINN MANUAL 1.0, *supra* note 28, at 47–52).

90. However, these activities may potentially violate the territorial sovereignty of a State. For additional discussion on this topic, see Garrie & Reeves, *supra* note 30, at 1857–58 (discussing how cyber actions that fall below the use-of-force threshold may still violate international law). Regardless, such actions would still be regulated by *Tallinn 2.0*. *See* TALLINN MANUAL 2.0, *supra* note 2, at 1 (noting *Tallinn 2.0*'s inclusion of "the public international law governing cyber operations during peacetime" in order to address "cyber issues that lie below the use of force threshold").

91. *See* TALLINN MANUAL 2.0, *supra* note 2, at 1 (noting that *Tallinn 2.0* is a "follow-on initiative to expand the Manual's scope to include the public international law governing cyber operations during peacetime").

92. *Id.* at 2–3. *Lex lata* is defined as "what the law is." J. Jeremy Marsh, Lex Lata *or* Lex Ferenda*? Rule 45 of the ICRC Study on Customary International Humanitarian Law*, 198 MIL. L. REV. 116, 117 (2008). *Lex ferenda* is defined as "what the law should be." *Id.*

93. *See* TALLINN MANUAL 2.0, *supra* note 2, at 3 ("[T]he Experts involved in both projects [*Tallinn 1.0* and *2.0*] assiduously avoided including statements reflecting *lex ferenda*."); Schmitt, *supra* note 5, at 271 ("Adding to the uncertainty regarding the precise legal parameters of cyber warfare is the fact that public international law is by nature a dynamic creature. . . . [I]ts content, interpretation, and application evolve over time in response to transformation of the security environment in which it applies.").

Chapter, created a foundational document with room for international law to develop and fill gaps as needed.[94] This "gap filler" will come in the form of either a treaty or by States' "engaging in practices out of a sense of legal obligation (*opinio juris*) that, combined with similar practice by other [S]tates, eventually crystallizes into customary international law."[95] With the accelerating pace of change in cyberspace[96] and the glacial speed at which conventional law develops,[97] new international law will likely come through State practice.

Although certain terms in the IHRL Chapter generally—and in Rules 36 and 37, specifically—are problematic, both the IHRL Chapter and the *Tallinn Manual 2.0* represent a tremendously useful starting point for assessing the challenging intersection of multiple areas of the law. Quickly filling definitional gaps is essential to amplifying the Chapter and determining what legitimate reasons may exist to violate rights, such as privacy, in cyberspace. Moreover, understanding timely, relevant activities not triggering the law of armed conflict but nevertheless of the type contemplated throughout *Tallinn 2.0*, such as the United States' C-ISR and C-OPE efforts, serve as tremendous indicators of State practice in this area.

Finally, it must be stated that the above nuanced criticism is not a broad condemnation of the Group of Experts' efforts in any regard. To the contrary, it is only because of their excellent and unprecedented work that we are able to spot the definitional gaps and begin to fill them with evidence of State practice. All of it, and especially the IHRL Chapter, represents a tremendous contribution to the law.

94. *See* Schmitt, *supra* note 5, at 299 ("International law is designed to govern the present and shape the future.").

95. *Id.* at 272–73 (citing Statute of the International Court of Justice art. 38(1), June 26, 1945, 59 Stat. 1055).

96. *See* DEFENSE REVIEW REPORT, *supra* note 28, at iii (discussing how the "pace of change continues to accelerate" in modern warfare).

97. *See* TALLINN MANUAL 2.0, *supra* note 2, at 3 ("There are very few treaties that directly deal with cyber operations and those that have been adopted are of limited scope.").

* * *

Interpretation Catalysts in Cyberspace

Rebecca Ingber*

Introduction

The cybersphere offers a rich space from which to explore the development of international law in a compressed time frame. Rapidly advancing capabilities and novel events distill and sharpen longstanding debates in international law: questions involving how the law adapts to new technologies; disagreement over the extent to which secret action can move custom;[1] disputes over the need for heightened transparency;[2] and power wrangling between states and soft law endeavors in driving the development of the law. In particular, the continuously evolving need to determine how existing laws apply to shifting capabilities provides fertile ground for innovative legal positioning and interpretation. That constant innovation in turn creates opportunities for discrete triggers for legal interpretation—or "interpretation catalysts" as I have termed them elsewhere[3]—to influence the path that legal evolution takes. Interpretation catalysts not only compel a decision-making body to take a position on its interpretation of a legal rule; they shape all aspects of the decision-making process, ultimately influencing the legal position that body takes, and often the resulting law itself.[4]

In this generative space of cyber law, the *Tallinn Manual* processes of the past ten years provide a valuable lens through which to witness the effects of interpretation catalysts on the evolution of international law. The *Tallinn* processes have been remarkable achievements, both in producing manuals that navigate the web of international laws regulating state action in cyberspace, and in driving states to consider and to continue to develop the rules governing this space. The two *Tallinn Manuals*[5] lay out for states not

---

* Associate Professor, Boston University School of Law. Many thanks to Susan Akram, Pamela Bookman, Daniela Caruso, Ashley Deeks, Kristen Eichensehr, Dustin Lewis, Dinah PoKempner, Naz Modirzadeh, Robert Sloane, and Phil Spector for invaluable conversations and comments on drafts. I am grateful to Stew Sibert for excellent research assistance.

1. Alexandra H. Perina, *Black Holes and Open Secrets: The Impact of Covert Action on International Law*, 53 COLUM. J. TRANSNAT'L L. 507, 511 (2015).

2. Harold H. Koh, *The Legal Adviser's Duty to Explain*, 41 YALE J. INT'L L. 189, 189–90 - (2016).

3. *See* Rebecca Ingber, *Interpretation Catalysts and Executive Branch Legal Decisionmaking*, 38 YALE J. INT'L L. 359, 360 (2013) (identifying the concept of "interpretation catalysts," and demonstrating their role in triggering distinct processes within the executive branch for formulating legal positions).

4. *Id.* at 377.

5. TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE (Michael Schmitt ed., 2013) [hereinafter TALLINN MANUAL]; TALLINN MANUAL 2.0 ON THE

only an experts' sense of where consensus on the law currently stands, but also—and just as importantly—the parameters of precisely where the disagreements among states may lie, where there might be room for movement, and what the outer parameters of that movement might be. And for academics, the *Tallinn* processes also provide a unique case study to consider the development of international law over a short period of time and the influence of soft law processes on that development.

In particular, the *Tallinn Manual* processes and resulting manuals provide insight into how these "interpretation catalysts," or discrete triggers for legal interpretation, influence the path that legal evolution takes.[6] The operative interpretation catalyst triggering the need for a legal decision influences every aspect of decision making from the identity of the particular players involved in an interpretative endeavor to the task before them, the context in which they operate, and the investment in the project by the relevant players.[7] In the *Tallinn* processes, those players have included not only the experts around the drafting table but also states watching and engaging from the sidelines. All of these factors shape where the law—or the interpretation of the law—ultimately lands.[8]

In prior work, I have explored the phenomenon of "interpretation catalysts" through the lens of state decision making, specifically U.S. executive branch legal decision making on matters of national security.[9] In that context, the lack of external checks on the U.S. President often means that the executive branch legal position is virtually the only operative legal constraint.[10] The interpretation catalyst driving such executive branch decision making therefore has an enormous influence not just on one party's opening legal position but on the governing law itself.[11]

In the case of the *Tallinn* processes, as I will elaborate in Part II, interpretation catalysts operate on two levels. The initial interpretation catalyst, the Estonia cyberattacks, impelled states to consider the applicable legal framework to apply to those attacks. Most significantly for our purposes, those events triggered the initiation and development of the first *Tallinn Manual* process itself, thus setting those wheels in motion.[12] Second, both *Tallinn* processes have themselves acted and continued to act as

---

INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS (Michael Schmitt & Liis Vihul eds., 2017) [hereinafter TALLINN MANUAL 2.0].

6. Ingber, *supra* note 3, at 377 (identifying and exploring the role of "interpretation catalysts" in driving decision making in the context of U.S. executive branch legal interpretation).

7. *See id.*

8. *See id.*

9. *See id.*

10. *See id.*

11. *Id.*

12. *See infra* notes 45–48 and accompanying text.

interpretation catalysts for states, compelling them—often intentionally—to develop their positions on the legal rules governing cyberspace. As I will touch on below as well, this case study illustrates not only how distinct events can trigger and shape the path of legal interpretation, but also that these triggers are not fixed; the power inherent in interpretation catalysts suggests that they may also be manipulated to push the law toward desired ends.

Now, I should acknowledge up front that the stated intent of the *Manual*'s drafters is not to drive the law but rather to lay out the current areas of legal consensus and of continued debate.[13] And yet the drafters also evince a clear intent to push states "proactively" toward development of the law themselves as well as in conjunction with the project.[14] A state legal adviser could not fail to notice that if states do not start working together to hammer out the rules governing this space, there is a risk these non-state-driven projects will continue to outpace them and ultimately may nudge the law in directions that states do not necessarily wish it to go.[15] It is for that very reason that the Dutch government sponsored "The Hague Process," a major convening of states, in order to review and comment on the *Tallinn Manual 2.0* while that process was underway.[16]

As states participating in The Hague Process no doubt concluded, it would be naïve to assume that the *Tallinn* processes would have no effect on development of the law. It is worth, then, pausing to consider the direction that such a project might push the law and indeed quite likely already has. I do not take a strong normative position in this piece on the specific direction cyber law has taken during the course of this project, other than to recognize the benefits of clarity in the law for state actors and others interested in the rule of law and in public law more generally. My intended contribution here

13. Michael Schmitt, Tallinn Manual 2.0 on the International Law of Cyber Operations: *What It Is and Isn't*, JUST SECURITY (Feb. 9, 2017), https://www.justsecurity.org/37559/tallinn-manual-2-0-international-law-cyber-operations [https://perma.cc/Z7ZA-QXKN].

14. *See id.* (explaining the virtues of clarity in the law regulating state action, in, *inter alia*, "lend[ing] stability to international relations" and "help[ing] deter other states from exploiting . . . grey zones in the law of cyberspace"); Tallinn Manual *Experts Meet for Intense Drafting Session*, NATO COOP. CYBER DEF. CTR. EXCELLENCE, 2:55–3:20 (Oct. 9, 2015), https://ccdcoe.org/tallinn-manual-20-be-completed-2016.html [https://perma.cc/EY2S-MKTD] (interviewing Tim McCormack, Professor of Law at the University of Melbourne, who explains that states are often "reactive to new . . . developments" and that *Tallinn 2.0* is an effort "to gather a group of experts together to proactively clarify the state of the law in an area that states are still asking questions about what law is going to apply").

15. *See* Schmitt, *supra* note 13 (noting that participants in the *Tallinn* process intended "that it would enhance the process of norm identification and elucidation by states"); Michael J. Adams, *A Warning About* Tallinn 2.0 . . . *Whatever It Says*, LAWFARE (Jan. 4, 2017), https://www.lawfareblog.com/warning-about-tallinn-20-. . .-whatever-it-says [https://perma.cc/92R7-RAM9] (expressing concern that users of the *Tallinn* manuals may inappropriately conclude that the law in certain areas is more settled than states have in fact themselves determined).

16. *See* Schmitt, *supra* note 13 (describing "The Hague Process").

is primarily to highlight the strong influence of the triggers for legal interpretation on decision-making processes, on the legal positions coming out of those processes, and thus, on the ultimate development of the law. The *Tallinn* processes—and specifically the second *Tallinn* process's treatment of international human rights law as contrasted with its treatment of the law of armed conflict—form an invaluable case study to examine the role of interpretation catalysts in legal interpretation.

I. Human Rights in Cyber Law

Both of the *Tallinn* processes and their ultimate products—the original *Tallinn Manual on the International Law Applicable to Cyber Warfare*,[17] released in 2013, and the *Tallinn Manual 2.0*, released this spring—are enormous undertakings and incredible achievements. The convener's intent for each, we are told in the *Tallinn 2.0* document itself, was to produce a handbook that would provide an "objective restatement of the *lex lata*" to actual practitioners, primarily "state legal advisers charged with providing international law advice to governmental decision makers, both civilian and military."[18]

I have no doubt that these state actors will indeed find the *Tallinn Manual 2.0* a useful resource. And it will be most useful to these state legal advisers and other practitioners *not* because, as some might assume, it provides flexible, expansive interpretations of the legal rules, which will lend them legal justification for whichever actions they wish to take in cyberspace; rather, it will be useful primarily to the extent it provides them with granular, specific answers regarding their legal obligations and constraints in areas where practitioners may seek clear guidance as to the appropriate legal space in which to operate.

Furthermore, *Tallinn 2.0* does not shy away from areas that might be most controversial for states, such as the role of international human rights law in constraining states' actions in cyberspace. In fact, it tackles this matter head-on and announces explicitly that "[i]nternational human rights law is applicable to cyber-related activities."[19] Despite the difficulty in finding consensus among the experts—not to mention the state participants in the

17. *See generally* TALLINN MANUAL, *supra* note 5.

18. TALLINN MANUAL 2.0, *supra* note 5, at 2–3; *see also* Rachel Ansley, *Tallinn Manual 2.0: Defending Cyberspace*, ATLANTIC COUNCIL (Feb. 15, 2017), http://www.atlanticcouncil.org/blogs/new-atlanticist/tallinn-manual-2-0-defending-cyberspace [https://perma.cc/UKC7-3YXG] (quoting Michael Schmitt: "We were not writing for academics. We were writing for countries.").

19. TALLINN MANUAL 2.0, *supra* note 5, at 182 (Rule 34). This statement is consistent with United Nations General Assembly's (UNGA) approach of the last several years. *See, e.g.*, G.A. Res. 68/167, ¶ 3 (Dec. 18, 2013) ("[T]he same rights that people have offline must also be protected online, including the right to privacy.").

process—in determining precisely how specific rules of human rights law operate in cyberspace and the disparity among states in acceptance of particular treaty regimes, the *Manual* firmly states that these rules act as constraints on states.[20] The *Manual* suggests no intent to evade human rights rules; quite the contrary, it suggests (and this is a stated goal of its leadership) an intent to place a marker for future actors to understand that human rights law provides constraints and to prompt them to determine precisely how these rules operate in context.[21]

And yet, despite this clear, human rights-embracing statement and intent, I predict the *Manual* will face some real criticism from the human rights community, and for good reason.[22] The human rights chapter is everything the handbook-style rules regulating state action under the use of force and law of armed conflict (LOAC) sections are not; the legal rules described in the human rights chapter are painted with broad brushstrokes, at a high level of generality, and thus, as I explain below, suggest greater flexibility for state discretion and potentially even evasion. Ultimately, the international human rights law (IHRL) rules laid out by the *Manual* simply provide insufficient clarity to be terribly useful to state legal advisers.

In a vacuum, there may be little danger in a document that simply restates a human rights obligation at a high level of generality. Here, the danger lies largely in the disparity between the human rights chapter and other critical sections of the *Manual*, in particular the significant discussions of the law governing the use of force and LOAC. The *Manual* holds itself out as providing the very clarity and granularity that is missing from the discussion of human rights. And experience suggests that the absence of that specificity may read to states as space or flexibility in the law.

I should include here some caveats. My observations—including that this particular *Manual* is predominantly engaged with the law governing the use of force and LOAC on a level of detail that it does not employ with

---

20. TALLINN MANUAL 2.0, *supra* note 5, at 182 (Rule 34).

21. *See* TALLINN MANUAL 2.0, *supra* note 5, at 182 (imposing obligation on states to conform to international human rights law in cyberspace despite recognizing that "state understandings concerning the precise scope of certain human rights entitlements in the cyber context . . . vary"); Michael Schmitt, Dir., Tallinn Manual 2.0 Project, Address at the Texas Law Review Symposium: Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Feb. 7, 2017). In interviews and writings, *Tallinn*'s director, Michael Schmitt, has explained that the goal of the *Manual* more broadly is to help "states focus their efforts where clarification of the law is needed and in their national interest." *E.g.*, Schmitt, *supra* note 13.

22. The *Manual* is only weeks old, but at least one commentator has raised concerns with its treatment of human rights. *See* Dinah PoKempner, Gen. Counsel, Human Rights Watch, Address at the Texas Law Review Symposium: Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Feb. 7, 2017); Dinah PoKempner, *Squinting Through the Pinhole: A Dim View of Human Rights from* Tallinn 2.0, 95 TEXAS L. REV. 1599, 1602 (2017); *see also* Adams, *supra* note 15.

respect to IHRL—are not intended as criticism of the actors involved here or even of the main approach of the *Manual*. I see two potential reasons for the disparity the *Manual* takes to these two bodies of law: One is actual ambiguity or lack of detail in IHRL and its relationship to cyberspace vis-à-vis LOAC.[23] Another is that the actors involved or the process itself led toward a disparate treatment of these two sections. There may be a bit of each at work here. But these may not be entirely separable factors. Considering the years-long first *Tallinn* process's focus on the rules of cyber *warfare*, we cannot entirely divorce any paucity in the law of human rights in cyberspace from the process's outsized focus on drilling into the laws of war. It may well be that the provenance of the *Tallinn* process gave the laws of war a head start.[24] In any event, as will be clear in my discussion of interpretation catalysts below, I see this disparity as an organic and potentially inevitable development given the original triggers for the project and the path its development has taken. At the end of this section, I will make a modest suggestion for how to address the concerns I raise here. But for now, let us dive into those specific concerns.

First, in order to understand how both state actors and human rights advocates might approach this manual, it is worth understanding some context regarding the relationship of states—in particular the United States—to international human rights law in the realm of conflict and national security. For years, U.S. human rights advocates, in particular, have sought to gain traction with the government on a broad range of matters dealing with conflict and security.[25] And yet there remains a perception—particularly

---

23. *See, e.g.*, Marko Milanovic, *Foreign Surveillance and Human Rights, Part 5: The Substance of an Extraterritorial Right to Privacy*, EJIL: TALK! (Nov. 29, 2013), https://www.ejiltalk.org/foreign-surveillance-and-human-rights-part-5-the-substance-of-an-extraterritorial-right-to-privacy/ [https://perma.cc/6WXQ-XTP2] (discussing the need to "flesh[] out" detailed rules governing an "extraterritorial right to privacy").

24. *See id.* (noting that detailing such rules "will happen in an iterative process").

25. As part of this effort, U.S. human rights organizations have over the course of the last decade and a half created divisions within their institutions specifically devoted to matters of war and national security. *See, e.g.*, *About the ACLU's National Security Project*, AM. CIV. LIBERTIES UNION, https://www.aclu.org/other/about-aclus-national-security-project [https://perma.cc/27CF-4E4U] (detailing the ACLU's "National Security Project," which was "[o]riginally created as an informal working group after the September 2001 attacks"); *see also Counterterrorism*, HUM. RTS. FIRST, http://www.humanrightsfirst.org/topics/counterterrorism [https://perma.cc/NA27-KAA4] (highlighting Human Rights First's work at the nexus of national security and human rights); *National Security*, HUM. RTS. WATCH, https://www.hrw.org/united-states/national-security [https://perma.cc/F9C4-3Z8G]; *National Security and Human Rights Campaign*, OPEN SOC'Y FOUND. (Sept. 18, 2013), https://www.opensocietyfoundations.org/grants/national-security-and-human-rights-campaign [https://perma.cc/7VGC-7PYJ]; *Security and Human Rights*, AMNESTY INT'L, http://www.amnestyusa.org/our-work/issues/security-and-human-rights [https://perma.cc/X6N5-G47P] (detailing the work of Amnesty International's U.S.-based affiliate with respect to national security and human rights); *U.S. National Security and Human Rights*, OPEN SOC'Y POL'Y

with respect to the U.S. government—that the law of international human rights has been sidelined in favor of a LOAC framework, LOAC expertise, and even LOAC-derived rules in contexts in which states have struggled to adapt international legal frameworks to new contexts. For example, through three very different presidential administrations, the U.S. government has applied the laws of war to its detention, targeting, and even surveillance operations in the conflict with al Qaeda and other groups.[26] Even when the government has found those rules difficult to map perfectly onto a conflict with a non-state actor, the government has retained a LOAC framework and reasoned by analogy to that body of law in determining the lawful space in which it could operate.[27]

Human rights experts, in the meantime, have repeatedly sought to push the government to accept and apply international human rights norms in this space and to bring U.S. policies in line with these rules.[28] Throughout the course of the Obama Administration, those efforts of human rights advocates, and the resulting tension with and within the Administration, in addition to pressure from allies, is part of what lay beneath Obama-era attempts to impose an additional layer of often human rights-derived policy prescriptions on top of the Administration's interpretation of its legal constraints on U.S. actions in a range of areas, such as the targeted killing realm.[29] In many of

---

CTR. (Feb. 24, 2017), https://opensocietypolicycenter.org/issues/u-s-national-security-human-rights/ [https://perma.cc/ZN6U-XF5P]

26. Hamdi v. Rumsfeld, 542 U.S. 507, 516 (2004); Respondents' Memorandum Regarding the Government's Detention Authority Relative to the Detainees Held at Guantanamo Bay at 1, *In re* Guantanamo Bay Detainee Litigation, 577 F. Supp. 2d 312 (D.D.C. 2008) (No. 08-442) [hereinafter March 13 Brief]; Rebecca Ingber, *Co-Belligerency*, 42 YALE J. INT'L L. 67, 74–80 (2017). While we do not yet have a definitive statement from the Trump Administration on its legal position on the framework for these conflicts with al Qaeda and other groups, all evidence suggests at a minimum that the Administration intends to continue a wartime framework. *See, e.g.*, Charlie Savage, *ISIS Detainees May Be Held at Guantánamo, Document Shows*, N.Y. TIMES (Feb. 8, 2017), https://www.nytimes.com/2017/02/08/us/politics/guantanamo-islamic-state-detainees.html?_r=0 [https://perma.cc/FBU9-55VW] (discussing a leaked draft executive order announcing the Trump Administration's potential policy of military detention for members of al Qaeda, ISIS, and other groups); Draft Executive Order on Protecting America Through Lawful Detention of Terrorists and Other Designated Enemy Elements (2017), https://assets.documentcloud.org/documents/3455640/Revised-draft-Trump-EO-on-detainees-and-Gitmo.pdf [https://perma.cc/K23D-DXFA] (characterizing, within a leaked draft of a Trump Administration Executive Order obtained by the *New York Times*, conflicts with Al Qaeda and other groups as a "continuing state of armed conflict with terrorist groups").

27. *See* March 13 Brief, *supra* note 26, at 1 ("Principles derived from law-of-war rules governing international armed conflicts, therefore, must inform the interpretation of the detention authority Congress has authorized for the current armed conflict.").

28. *See, e.g.*, Alfred de Zayas, *Human Rights and Indefinite Detention*, 87 INT'L REV. RED CROSS 15, 37 (2005) (rejecting "indefinite detention" as unlawful under international human rights law).

29. Press Release, Office of the Press Sec'y, White House, Fact Sheet: U.S. Policy Standards and Procedures for the Use of Force in Counterterrorism Operations Outside the United States and

these areas, however, the Obama Administration did not alter those underlying legal positions, which were largely a holdover from the prior Administration's decision to treat the conflict in LOAC terms.[30] As a matter of *law*, the Obama Administration also generally retained a variety of legal tools—including the concept of "*lex specialis*" and the position that many human rights treaties were not intended to apply extraterritorially, both of which I will discuss in more detail below—that together entailed an evasion of a strict application of specific human rights rules onto many of its activities in this space.[31] The result in certain areas was a human rights policy overlay on top of a LOAC legal framework, an outcome Naz Modirzadeh has criticized as blurring the lines between genuine legal rules and the policies governing state action.[32] This recent history is an important backdrop against which to examine and understand the *Tallinn Manual 2.0*'s approach to human rights in cyberspace.

The most immediate, and perhaps striking, thing one notes in reviewing the IHRL chapter, particularly in light of the background that I just surveyed,

---

Areas of Active Hostilities (May 23, 2013), https://obamawhitehouse.archives.gov/the-press-office/2013/05/23/fact-sheet-us-policy-standards-and-procedures-use-force-counterterrorism [https://perma.cc/Z2BM-VA39] (explaining the policy overlay of procedural safeguards, as well as near-certainty requirements and a preference for capture over kill, for targeting operations).

30. *See* Ashley S. Deeks, *The Obama Administration, International Law, and Executive Minimalism*, 110 AM. J. INT'L L. 646, 646–47 (2016) (arguing that the expansion of power under the Bush Administration enabled the Obama Administration to take a more minimalist approach without sacrificing any of the legal powers gained in the Bush years); Rebecca Ingber, *The Obama War Powers Legacy and the Internal Forces that Entrench Executive Power*, 110 AM. J. INT'L L. 680, 681–82 (2016) (arguing that internal features of the executive branch lead to the retention of legal authorities by the President from one administration to the next).

31. *See, e.g.*, WHITE HOUSE, REPORT ON THE LEGAL AND POLICY FRAMEWORK GUIDING THE UNITED STATES' USE OF MILITARY FORCE AND RELATED NATIONAL SECURITY OPERATIONS 34 (2016), https://www.justsecurity.org/wp-content/uploads/2016/12/framework.Report_Final.pdf [https://perma.cc/R664-YKZE] ("In accordance with the doctrine of *lex specialis*, where these bodies of law conflict, the law of armed conflict would take precedence as the controlling body of law with regard to the conduct of hostilities and the protection of war victims. However, . . . armed conflict does not automatically suspend [o]r . . . displace the application of all international human rights obligations."); Marko Milanovic, *Harold Koh's Legal Opinions on the US Position on the Extraterritorial Application of Human Rights Treaties*, EJIL: TALK! (Mar. 7, 2014), http://www.ejiltalk.org/harold-kohs-legal-opinions-on-the-us-position-on-the-extraterritorial-application-of-human-rights-treaties/ [https://perma.cc/YG99-NTUK] (discussing reports of leaked opinions by then-State Department Legal Adviser Harold Koh advising the U.S. Government to change its position on the extraterritorial application of its ICCPR and CAT obligations); Beth Van Schaack, *United States Report to the UN Human Rights Committee: Lex Specialis and Extraterritoriality*, JUST SECURITY (Oct. 16, 2013), https://www.justsecurity.org/1761/united-states-lex-specialis-extraterritoriality/ [https://perma.cc/R84E-CM44] (laying out the recent history of the U.S. position on *lex specialis* and extraterritoriality of its ICCPR obligations before the Human Rights Committee).

32. Naz K. Modirzadeh, *Folk International Law: 9/11 Lawyering and the Transformation of the Law of Armed Conflict to Human Rights Policy and Human Rights Law to War Governance*, 5 HARV. NAT'L SECURITY J. 225, 228–30 (2014).

is that its overarching tone is quite friendly to the application of IHRL in cyberspace. The very first rule states firmly and clearly that "[i]nternational human rights law is applicable to cyber-related activities."[33] This written statement accords with the stated intent of the directors of the project, who have noted that their objective in this chapter was to alert state legal advisers of the need to grapple with their state's human rights obligations in this realm.[34] To the extent the simple alerting of legal advisers to the need to address a body of law is the goal, the chapter itself accomplishes this, and perhaps need not have even moved on from that initial rule.

But the chapters of this *Manual* cannot each be read in a vacuum; they exist and will be read alongside the rest of the work as a whole. And when one examines the *Manual* in its entirety, there is a stark contrast between the approach taken in the human rights chapter and that of the other content of the handbook, in particular the nearly 250 pages of direct discussion of LOAC plus additional content threaded throughout the *Manual*. The immediate impression, to say the least, is that human rights law was not the focus of this project.

Now, the fact that a soft law project focuses on one area of law at the expense of or in lieu of another is itself neither an error nor a flaw. Nevertheless, to the extent the project is held out as an overarching manual covering the waterfront on all issues involving cyberspace that may arise for a state, it is important to highlight the contrasting approaches to these different bodies of law and flag some potential hazards, particularly for states looking to this *Manual* as the definitive work on the international law governing cyberspace. In particular, and considering the backdrop I laid out at the start of this section, there are some flags here that suggest state actors might rely upon the human rights chapter as a justification for discretion rather than as a source of clear constraint. I will discuss a few of these here.

A. Confinement of the Human Rights Chapter to a Narrowly Defined Geographic Space in the Manual

One concern with the approach the *Manual* takes to human rights is geographic—both in form and substance. Discussion of human rights in the *Manual* is primarily confined to the human rights chapter—which is itself a relatively short 30 pages in an over 600-page manual, of which about half is devoted to the laws of war.

There are a number of alternative approaches the *Manual* drafters might have taken to address the role of human rights law in this space. A more

33. TALLINN MANUAL 2.0, *supra* note 5, at 182 (Rule 34).

34. Schmitt, *supra* note 13; *see also* Michael N. Schmitt & Liis Vihul, *Respect for Sovereignty in Cyberspace*, 95 TEXAS L. REV. 1639, 1640–41 (2017).

human rights-focused approach might have been to weave human rights law norms and rules throughout the discussion, in each of the sections, as different scenarios are contemplated, as is done throughout with LOAC.[35] It is not clear to what extent human rights experts who drafted or reviewed the human rights chapter were also involved in the work of the rest of the *Manual* or to what extent they were able to weigh in on each and every rule throughout. But a human rights-driven approach might have resulted in a discussion of how human rights law regulates, for example, how a state may engage civilians who participate in acts of hostilities during armed conflict; or the concept of collective punishment; the rule about cyber booby traps; contemplation of a state's duty to protect cyber infrastructure; or cyber interference with telecommunications; each of which could readily benefit from a discussion of how human rights law also regulates state actions in such circumstances.[36]

Instead, the *Manual* relegates the discussion to a chapter within a larger section marked "specialised regimes," alongside primarily *geographically-focused* legal regimes—like the seas, outer space, and diplomatic premises.[37] Though this was not necessarily intended, a reasonable inference to draw from that placement is that IHRL is a body of law parallel to those specialized regimes. One might be forgiven for assuming that it only exists in some kind of confined geographic space. Of course, the view that a state's human rights law obligations are entirely constrained by geography and inoperative beyond that state's legal borders does exist, and lies on one extreme side of the debate over the extraterritorial application of human rights law. Notably, it is a view that *the Manual itself does not espouse*.[38] Nevertheless, the confined geographic location in the *Manual* seems to reflect a residual sense of human rights law as belonging to a wholly separate and confined space, which belies the complexity of state positions on how they see and apply their obligations outside their borders. And it might help entrench such an impression for state legal advisers relying upon the *Manual* as a guide.

---

35. *See, e.g.*, TALLINN MANUAL 2.0, *supra* note 5, at 53 (discussing the interplay between jurisdiction, LOAC, and *Tallinn 2.0* Rule 8); *id.* at 74 (discussing how LOAC affects foreign state immunities with respect to *Tallinn 2.0* Rules 44, 82, and 152); *id.* at 127 (discussing the interaction between countermeasures, LOAC, and *Tallinn 2.0* Rules 23, 72, 92, and 113).

36. *Id.* at 217 (discussing the duty to protect cyber infrastructure under Rule 40); *id.* at 288 (discussing the duty to safeguard international telecommunication infrastructure under Rule 61); *id.* at 294 (discussing harmful interference with non-military cyber services under Rule 63); *id.* at 428 (discussing civilian direct participants in hostilities under Rule 97); *id.* at 457 (discussing cyber booby traps under Rule 106); *id.* at 539 (discussing collective punishment under Rule 106). This is not to say the *Tallinn Manual 2.0* is entirely devoid of human rights references outside of that chapter; the *Manual* does include throughout some limited cross-referencing to the human rights chapter, though nowhere near as extensively or fluidly as it interweaves the discussion of LOAC.

37. TALLINN MANUAL 2.0, *supra* note 5, at vi–vii.

38. *Id.* at 183–87.

B. Lex Specialis

Another flag for state actors is the *Manual*'s discussion of *lex specialis*.[39] The *Manual* states that the "precise interplay between [LOAC] and [IHRL] remains unsettled," but that under the concept of *lex specialis*, the laws of war will often comprise the more specific rules to apply to armed conflict.[40] There is much packed into that brief statement, and it must be read in light of the context I discussed above, in which—whether there is merit to this approach or not—the concept of *lex specialis* has long been applied by the states to assert formal compliance with human rights law, while evading their specific application to wartime activities. In this case, by not laying out precisely how this rule of *lex specialis* will apply in individual situations, the *Manual* risks suggesting to states that they have significant discretion to disregard human rights rules in armed conflict by pointing to "more specific" LOAC rules. As I will discuss in the section that follows, the *Manual* itself then lays out these LOAC rules in careful detail.

C. Lack of Granularity in the Human Rights Rules

A concern that goes hand in hand with the problem of *lex specialis* is the lack of granularity in the rules announced in the human rights chapter. As I mentioned, this chapter opens with an overarching statement that is quite favorable to the role of human rights in regulating state action. Yet each of the rules listed in the chapter is so high-level or vague as to be fairly anodyne in its practical suggestion of constraints on state action.

Consider how the *Manual* might have treated differently even just the substantive areas that it lists under Rule 35, "[i]ndividuals enjoy the same international human rights with respect to cyber-related activities that they otherwise enjoy."[41] Each of these distinct substantive areas, from freedom of expression to privacy to due process, might itself be its own rule, or even its own chapter. This is not for lack of an interest in granularity by the *Manual* itself. Consider the *Manual*'s treatment of any LOAC rule as a comparison. Compare this broad rule, "[i]ndividuals enjoy the same international human rights with respect to cyber-related activities that they

---

39. *Id.* at 181.

40. *Id.* The *Manual* cites for this concept the International Court of Justice Nuclear Weapons advisory opinion, which states that while human rights obligations do not generally "cease in times of war," the interpretation of those obligations is "determined by the applicable *lex specialis*, namely, the law applicable in armed conflict which is designed to regulate the conduct of hostilities." Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226 (July 8).

41. TALLINN MANUAL 2.0, *supra* note 5, at 187.

otherwise enjoy,"[42] with, for example, Rule 105 prohibiting indiscriminate means or methods:

> It is prohibited to employ means or methods of cyber warfare that are indiscriminate by nature. Means or methods of cyber warfare are indiscriminate by nature when they cannot be: (a) directed at a specific military objective, or (b) limited in their effects as required by the law of armed conflict and consequently are of a nature to strike military objectives and civilians or civilian objects without distinction.[43]

Or Rule 132 on medical computers:

> Computers, computer networks, and data that form an integral part of the operations or administration of medical units and transports must be respected and protected, and in particular may not be made the object of attack.[44]

Or Rule 122 on perfidy:

> In the conduct of hostilities involving cyber operations, it is prohibited to kill or injure an adversary by resort to perfidy. Acts that invite the confidence of an adversary to believe that he or she is entitled to, or is obliged to accord, protection under the law of armed conflict, with intent to betray that confidence, constitute perfidy.[45]

First, the broad human rights rule is phrased as a contingent standard: it is a rule that depends entirely on a state's view of its human rights obligations in other spheres. The LOAC rules, by contrast, are stated as hard prohibitions.

Moreover, the human rights rule operates at a very high level of generality, whereas the LOAC rules are not only noncontingent, they are highly specific. Particularly when viewed alongside such granular LOAC rules, the high level of generality in the human rights chapter may suggest to states that they have significant discretion in how to engage their human rights obligations. For legal advisers who pick up the *Manual* to determine what they need to tell their clients in a particular scenario, these rules may not provide sufficient specificity to be of much use beyond a general notice that there is another potential body of law operating in this realm.

Moreover, the juxtaposition in the *Manual* of highly detailed LOAC rules against a vague, high-level discussion of human rights rules must be considered in light of the *lex specialis* issue I discussed above. Considering the *Manual*'s restatement of the *lex specialis* concept that the more specific rule governs, the *Manual*'s severe disparity in its treatment of human rights

---

42. *Id.* Note that this statement itself was not particularly groundbreaking, considering states have affirmed such a statement through United Nations General Assembly resolutions since 2013. *See, e.g.*, G.A. Res. 68/167, *supra* note 19.

43. TALLINN MANUAL 2.0, *supra* note 5, at 455.

44. *Id.* at 515.

45. *Id.* at 491.

law in relation to LOAC rules could easily be read to suggest that the LOAC rules are in fact more "specific" in each case, and thus that they crowd out the IHRL rules, rather than an alternative possibility: that the *Manual* simply did not drill down into—or compel states to develop through the course of two *Manual* processes—each potential principle of human rights law as it applies in the cyber context.

Rather than provide a bona fide handbook on the application of human rights law to cyberspace, this chapter reads as more of a placeholder. The intimation is: international human rights law is real, it is important, and it regulates state action even in this realm . . . and good luck figuring out how to apply it.

D. Methodology

Finally, and perhaps most importantly, even the methodology of the *Manual* itself appears constructed through the lens of use-of-force- and LOAC-based systems of legal rules, and is thus inadvertently weighted against deriving granular rules from human rights law. As the *Manual* explains, the process for adopting rules involved a requirement of consensus among the "International Group of Experts" that a rule reflected customary international law.[46] As such, the rules would be "binding on all states, subject to the possible existence of an exception for persistent objectors."[47] At times, a treaty text might itself "represent[] a reliable and accurate restatement of customary international law,"[48] according to the experts, in which case the *Manual*'s rule will resemble the treaty text.

This approach makes sense in the LOAC context, where state governments largely drive legal interpretation, and where there is a good deal of customary international law, as well as near-universal adoption of many significant treaties such that many are now taken to represent customary international law.[49] That widespread adoption of many treaty regimes and

---

46. TALLINN MANUAL 2.0, *supra* note 5, at 4.

47. *Id.*

48. *Id.*

49. *See, e.g.*, Geneva Convention Relative to the Treatment of Prisoners of War, Aug. 12, 1949, 6 U.S.T. 3316, 75 U.N.T.S. 135; 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; Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Victims of International Armed Conflicts, June 8, 1977, 1125 U.N.T.S. 4; Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Victims of Non-International Armed Conflicts, June 8, 1977, 1125 U.N.T.S. 609 (the United States is a signatory of both Additional Protocols but is currently one of very few states which have not yet ratified either); *see also Customary Law*, INT'L COMMITTEE RED CROSS, https://www.icrc.org/en/war-and-law/treaties-customary-law/customary-law [https://perma.cc/26PV-2BTR]. For the long list of treaties applicable to wartime, see *Treaties, States Parties and Commentaries*, INT'L COMMITTEE RED CROSS, https://ihl-databases.icrc.org/ihl [https://perma.cc/2U63-4J8H].

the deep core of customary international law mean that a project to determine the LOAC rules applicable to cyberspace can address a universal set of rules applicable to virtually all states without undermining the entire project.

By contrast, the international human rights legal regime, as Dinah PoKempner addresses in her piece, is heavily treaty-based, and elaborated through a wide array of governmental, quasi-governmental, and even *non*governmental mechanisms.[50] A methodology that is geared toward addressing only those rules that are universally applicable as customary international law or through nearly universally ratified treaties will highly underrepresent the plethora of treaty rules with which any given state is obligated to comply. Likewise, a methodology based solely in rules universally accepted by states misses the disparate array of enforcement mechanisms states face, which play large and differing roles in expounding human rights norms. The *Manual* makes a quick reference to part of this dilemma in the introduction, stating that "[u]sers of this Manual are cautioned that states may be subject to additional rules of international law set forth in treaties to which they are Parties."[51] But the universal and state-driven approach of the *Manual* provides yet another reason for the disparity in granular rules in the human rights section as compared to the rest of the *Manual*.

***

To conclude this section, it is very possible that a simple highlighting of human rights as another set of obligations states will need to address may very well be what the *Manual* drafters intended, or all they felt they could provide, when confronted with an area on which they could not reach consensus, or where there is still much work to do to develop how to apply the law in practice. And from the perspective of those who care about protecting human rights—as I gather the *Manual* experts do—a manual that exhorts its audience to consider human rights law is likely better than a document that ignores it altogether, or much worse, states that this body of law has no place in regulating cyber law. Nevertheless, the *Manual*'s approach to human rights is a far cry from the truly detail-oriented, practitioner-focused handbook that it serves as for other areas of law, particularly for the laws governing the use of force and armed conflict. And

---

50. PoKempner, *supra* note 22, at 1602 (stating that "nongovernmental experts, practitioners, and scholars have for decades provided much of the 'gas' in the 'engine' of human rights law mechanisms, be they treaty bodies, courts, review conferences, U.N. or regional procedures, or legislatures, and not only through the supply of relevant facts, but through legal analysis and interpretation").

51. TALLINN MANUAL 2.0, *supra* note 5, at 4. Interestingly, the *Manual* does at times point to specific treaty rules of LOAC as applicable to only those states that are party to the treaty. *See, e.g.*, *id.* at 481 (stating under Rule 118, Choice of Targets, "[f]or States Parties to Additional Protocol I, when a choice is possible between several military objectives for obtaining a similar military advantage, the objective to be selected for cyberattack shall be that the attack on which may be expected to cause the least danger to civilian lives and to civilian objects").

that disparity might leave operators with the impression that the rules of international human rights law governing cyberspace truly are undefined and, therefore, highly permissive.

All of this suggests that either human rights law simply was not the focus of this project, or that the experts viewed the state of human rights law as not as well-developed as the rules of LOAC as applied to the cyber realm (or both). If the former, this could be addressed by simply clarifying this early in the *Manual* itself—including front and center in the chapter addressing human rights. Otherwise, the *Manual* risks leaving readers with the impression that the latter—a lack of clarity in the law—is the cause for this disparity.

And if that is the case, if the experts running this process simply found that human rights law as applied to cyberspace was less well-developed than the laws of LOAC, then one has to wonder if that is not itself at least in part a function of the fact that the *Tallinn* project took one path from the start and not another. Considering that this decade-long process has been, after all, a project aimed at developing an understanding of where the law stands, and simultaneously at pushing states to develop that law themselves,[52] the experts leading the first *Tallinn Manual* project on the laws of cyberwarfare could rightfully consider themselves to have succeeded if that process in fact compelled states to develop clarity on how LOAC applies in the cyber realm.

As the next section will elaborate, I see the *Manual*'s approach to the human rights chapter as an organic and perhaps inevitable result of the initial trigger for the project itself, which defined the process taken to reach this ultimate result. If this result was driven by the process, the solution cannot easily lie in simply editing or lengthening the chapter itself, or in drilling down more concretely into the human rights rules within the context of the same process. Perhaps the only real option for human rights scholars and practitioners is to take up the task themselves, and draft a human rights-focused manual through a human rights-driven process. For the *Tallinn Manual* itself, however, it would be worth announcing a strong caveat to explain that the methodology, expertise, and direction of the process were not targeted toward the practice and mechanisms of the international human rights legal system, and should not be understood to represent the whole of *lex lata* in that space.

II. Interpretation Catalysts and Cyber Law

So how did it come to pass that a manual intended to provide clarity for states on rules regulating and constraining their action in cyberspace, may inadvertently provide states with a heightened sense of discretionary

52. *See* Schmitt, *supra* note 13 ("Those who participated in the seven-year Tallinn Manuals' journey hoped only that it would enhance the process of norm identification and elucidation by states.").

flexibility and potentially even—at the most cynical level—tools for evading the application of those rules in the area of international human rights law?

To understand this, we need to consider the context in which the original *Tallinn* process was born, sponsored, drafted, and ultimately published, and then served as the backdrop against which the *Tallinn 2.0* drafters operated.

As I note above, I have written elsewhere that the specific triggers for states' interpretations of the legal rules that bind them have a strong influence on their ultimate legal positions. These "[i]nterpretation catalysts can drive [states] to crystallize a legal view on a matter that is entirely novel; can bring a formerly identified but dormant issue into urgent focus; and can transfer an issue from one decision-making forum to another."[53] Interpretation catalysts influence decision making not only by forcing states to articulate a legal position, but in shaping the process through which states reach that decision, "including by determining a particular question's point of entry within the government, framing the task, shaping the interpretive process, establishing the relative influence of the relevant actors, and informing the contextual pressures and interests that may bear on the decision."[54] For example, the state's process for determining its legal position on the rules governing treatment of military detainees might differ dramatically depending on whether the state must first consider its public legal position within the context of drafting briefs in defensive litigation, or instead, in preparation for a hearing before a human rights treaty body.[55] The actors around the decision-making table; the process for reaching a decision; the identities of the actors holding the pen in drafting the specific language as well as the ultimate decider if consensus cannot be reached; the biases; contextual pressures; and time frame against which the decision makers act—all of these factors have a significant influence on the ultimate position the state takes.[56] And all of these factors are driven and defined by the initial "interpretation catalyst" for that decision.

In the case of the *Tallinn* processes, interpretation catalysts have operated on two levels: first, in prompting the creation of and direction for a group of experts seeking to define legal rules as guidance for state actors; and second, in prompting states themselves to participate in and receive guidance from that expert-led process. At the first level, the Estonia cyberattacks not only triggered the initial decision to channel legal decision making into a particular expert-led process; that initial catalyst also defined the creation of the entire process and the context in which the body of experts originated and defined their initial roles. In contrast to the influence of interpretation catalysts on the decision-making processes of a preexisting body, such as a

53. Ingber, *supra* note 3, at 360.

54. *Id.* at 360–61.

55. *Id.* at 390.

56. *Id.*

state, the catalyst that triggered the *Tallinn* process could have an even more powerful effect on the resulting decision-making process and positions, because it could influence everything from the ground up, including the constitution and mandate of this new entity.

At the second level, the *Tallinn* processes themselves have functioned as interpretation catalysts, triggering states to engage in legal positioning in response. The *Tallinn* processes have—and have intentionally—impelled states to engage in a rule-definition process on the terms and timing of the *Tallinn* expert-led groups. And those terms and timing included tackling a first-stage, law-of-war-driven project, *Tallinn 1.0*, before taking on the broader process of *Tallinn 2.0*.

A. Interpretation Catalysts at Stage One

Given the significance I place on the initial catalyst for interpretation, a critical—perhaps the most critical—publicly-known piece of this history is the trigger for the *Tallinn* process itself: the cyberattacks on Estonia in 2007, in which large portions of the country's cyber infrastructure—specifically government websites, banks, and Estonian news outlets—were essentially shut down for about three weeks as a result of massive distributed denial of service attacks.[57] These events raised a broad range of legal questions, many domestic, such as how Estonia's penal laws applied to actions in cyberspace, and its rules governing surveillance.

But on the international plane, the governments of Estonia and other states were concerned primarily about questions of state attribution, the range of lawful responses available, and what activities could be or even *must* be taken by Estonia's international allies, including whether Estonia might invoke NATO's Article 5 provisions regarding collective self-defense.[58] Estonia in particular had an incentive to conceive of those events in war terms, considering NATO's mutual defense obligations. For that reason or others, there was a felt need among affected states to understand the legal parameters for how international law rules governing conflict apply in the cyber context, and a pressing need, driven partly by state interest, to understand when and the extent to which such events might rise to the level of a use of force or armed attack. Focusing on how the laws of war in

57. Joshua Davis, *Hackers Take Down the Most Wired Country in Europe*, WIRED (Aug. 21, 2007), https://www.wired.com/2007/08/ff-estonia [https://perma.cc/9UL2-98JZ].

58. *See* TALLINN MANUAL 2.0, *supra* note 5, at xxiii (stating, in an introductory note by the current President of Estonia, that the 2007 cyberattacks against Estonia "sped up the establishment of the NATO Cooperative Cyber Defence Centre of Excellence" and that among the center's first activities was to commission the study that became *Tallinn 1.0*); TALLINN MANUAL 1.0, *supra* note 5, at 1 (stating, in a note by Michael Schmitt, that the original *Tallinn Manual* project gathered international law practitioners and scholars in order to "examine how extant legal norms applied to this 'new' form of warfare").

particular might operate in cyberspace was, therefore, partly driven by the reality of external events and partly driven by an interest in viewing those events through that wartime lens. As additional cyberattacks followed worldwide, with relevant states finding themselves on both the defensive and offensive ends of such acts, the need to address a baseline set of rules became apparent.[59]

The first *Tallinn Manual* was born out of this rising awareness about the need to come to terms with how international law regulates state action in the cyber realm. That this first project, *Tallinn 1.0*, focused on cyber *warfare*, and not on cyberattacks that do not meet a use-of-force threshold or on cyber security more broadly, can be traced to this initial trigger for the project. It can be traced to the needs of the Estonian government in particular but also to NATO allies' interests in contemplating their own engagement in those events and to the military nature of the organization that ultimately funded, hosted, and facilitated the process, NATO's Cooperative Cyber Defence Centre of Excellence (CCD COE). The first *Tallinn* process thus collected law-of-war expertise, under the auspices of the CCD COE, in order to seek to define the actual state of the laws of war in cyberspace as they existed at that time.[60]

Following the successful conclusion of the *Tallinn 1.0* process, the project immediately turned toward tackling the broader array of law applicable to peacetime cyber activities. The leaders of the *Tallinn* process recognized that the specific expertise necessary for the first *Tallinn* project on cyber warfare would not be sufficient for the broader scope of *Tallinn 2.0*. Thus, they expanded the team and, while retaining the same leadership, brought in an almost entirely new group of legal experts with backgrounds involving not just the law of armed conflict, but also diplomatic law, the law of the sea, space law, and, as we have discussed, human rights. Moreover, the *Manual* notes that care was taken to send individual chapters out to "experts in the respective subjects" to "prepare[] initial drafts of the rules and commentary," as well as to seek peer review by experts at later points on drafts of the *Manual*.[61]

Yet in broadening the group of experts and expertise—and this is of course only conjecture—the process may have encountered increased friction the second time around in coming to consensus on even what applicable body of law to apply to a particular context, let alone the precise contours of the legal rule. While surely a group of experts in any single field will have areas

59. *See* TALLINN MANUAL 1.0, *supra* note 5, at 1–2 (discussing the increase in cyber warfare after the 2007 cyberattack on Estonia, specifically citing the 2008 cyberattacks against Georgia and the 2010 "Stuxnet" cyberattack against Iran).

60. *Id.* at 1; *Manual 2.0 to Be Completed in 2016*, NATO COOP. CYBER DEF. CTR. EXCELLENCE (Oct. 9, 2015), https://ccdcoe.org/tallinn-manual-20-be-completed-2016.html [https://perma.cc/D4TN-DZXU].

61. TALLINN MANUAL 2.0, *supra* note 5, at 6.

of disagreement, there are also likely to be significant areas of consensus among actors within a shared field, and more so than there might be if views were instead solicited from a broader array of experts from multiple fields. Thus one can readily imagine that a group of, say, LOAC experts may find more avenues for agreement with respect to how LOAC might apply to a novel context, than would a more diverse group of experts drawn from disparate fields of expertise in seeking consensus on the applicability of rules from any given field. If my instincts are correct, *Tallinn 2.0* was as a whole bound to result in broader brushstroke, less granular rules than *Tallinn 1.0*, based on the simple reality of having to seek agreement and enshrine rules on the basis of the lowest common denominator, in a group of more diverse expertise.

If *Tallinn 2.0* were the whole of the project, a more high-level set of principles than those arising from *Tallinn 1.0* might have been the result of the process across the board. Yet the second *Manual* could not escape its ancestry. *Tallinn 2.0* could not but inherit the granular in-the-weeds assessment of LOAC rules as they apply in cyberspace, crafted in the *Tallinn 1.0* process. In updating the *Manual* with a broader group of experts, *Tallinn 2.0* may have updated the LOAC rules, but they and states had been living with the first manual in existence at this point for four years, and the second group of experts would not have seen themselves as having a mandate or need to water them down for the purpose of leveling the playing field with other fields of law in *Tallinn 2.0*. The result—quite possibly the *inevitable* result—is a manual that includes highly granular rules of LOAC, drawn from the first process, alongside more high-level principles applicable in other areas of law.

Were the *Manual* to be read in a vacuum, without an understanding of its history, one would be forgiven for assuming that these other bodies of law are simply less fleshed out, less determinate, in their application to cyberspace. And many of them likely are. Nevertheless, had the process begun with a different focus, not LOAC but a different field of law, it is likely that a homogenous group of experts (and by homogenous I mean in expertise, not in beliefs), in *any* of the fields addressed in the *Manual*, would be better able to reach consensus on the application of their field of expertise to cyberspace than would a body drawn from diverse areas of expertise. And the process itself would have impelled states to consider and develop the application of law in that field, just as the *Tallinn Manual 1.0* authors intended in the LOAC space.

Consider a thought experiment. Imagine that the trigger—the "interpretation catalyst"—prompting experts from Europe and the United States and elsewhere to come together to determine the applicable rules governing cyberspace were not the attacks on Estonia, but instead an event resulting in public and governmental outcry against state surveillance of personal communications. What if the public revelations of Angela Merkel's

tapped phone,[62] for example, had instead been the catalyst for this process? At the time of those revelations, states grappled with their response, weighing condemnation of the United States, while simultaneously facing new spotlight on their own surveillance measures.[63] Just as with the use-of-force and law-of-war questions that puzzled states in the aftermath of the Estonia attacks, surveillance too has raised thorny questions regarding the balancing of states' positions on both the offensive and defensive end of such measures.

Had those events instead been the catalyst for this soft law process, we quite likely would have seen a very different group of experts gather to discuss international cyber law, focused primarily on a very different set of core issues.[64] This "Berlin Manual 1.0," as we might have called it, might have focused solely on that initial range of surveillance issues and not attempted to go beyond, just as *Tallinn 1.0* cabined itself to cyber warfare. An entirely different array of experts would have been convened to tackle such issues. They would have taken a methodological approach appropriate to their expertise and to the substantive matter before them. A group of human rights experts, for example, might have started from a perspective of applying treaty rules to cyberspace, rather than starting with customary international law, and might have given more weight to the views of courts,

---

62. Mark Mazzetti & David E. Sanger, *Tap on Merkel Provides Peek at Vast Spy Net*, N.Y. TIMES (Oct. 30, 2013), https://nyti.ms/2lqLFPJ [https://perma.cc/N2N8-UEHZ].

63. *See, e.g.*, Michael Crowley, *Spies Like Us: Friends Always Spy on Friends*, TIME (Oct. 31, 2013), http://swampland.time.com/2013/10/31/friends-always-spy-on-friends/ [https://perma.cc/YV34-V4JK] (discussing the prevalence of international spying on allies); Ashley Deeks, *The Increasing State Practice and Opinio Juris on Spying*, LAWFARE (May 6, 2015), https://www.lawfareblog.com/increasing-state-practice-and-opinio-juris-spying [https://perma.cc/BKV2-FGM8] (recalling Germany's reaction to the Snowden revelations in light of the discovery of German surveillance); Melissa Eddy, *Germany Drops Inquiry Into Claims U.S. Tapped Angela Merkel's Phone*, N.Y. TIMES (June 12, 2015), https://nyti.ms/2lebJLy [https://perma.cc/HU3X-8H2X] (describing the German investigation into the allegations and the ultimate withdrawal of the investigation).

64. In the course of the last four years, numerous other processes have in fact been convened worldwide to examine and attempt to define the rules governing cyber activities in a broad range of areas, and these are in various stages of implementation. These include the following: African Union Convention on Cyber Security and Personal Data Protection, June 27, 2014, AU Doc. EX.CL/846(XXV), https://ccdcoe.org/sites/default/files/documents/AU-270614-CSConvention.pdf [https://perma.cc/2DLR-8GQC]; U.N. General Assembly, Letter dated Jan. 9, 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan, and Uzbekistan to the United Nations addressed to the Secretary-General, U.N. Doc. A/69/723 (Jan. 13, 2015) (introducing the Draft International Code of Conduct for Information Security, authored under the auspices of the Shanghai Cooperation Organization); Organization of American States Res. AG/RES. 2004 (XXXIV-O/04), Appendix A (June 8, 2004), http://www.oas.org/xxxivga/english/docs/approved_documents/adoption_strategy_combat_threats_cybersecurity.htm [https://perma.cc/6CSR-3UCQ]; High Representative of the Eur. Union for Foreign Affairs & Security Policy, *Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions*, JOIN (July 2, 2013), http://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf [https://perma.cc/9ACF-Q9UT].

U.N. bodies, and a plethora of other nongovernmental and inter- or quasi-governmental actors.[65] There would have been no shortage of debate about how the rules applied, as surely there was among the law-of-war experts, but a multi-year process would have ultimately yielded some granular set of rules specific to that body of law, and simultaneously pushed the development of the law toward greater specificity as well.

If the "Berlin Manual" were a success, as was *Tallinn 1.0*, we can imagine there would have been clamor for a new manual to cover a broader range of issues. The second process, if it were run like *Tallinn 2.0*, would likely take on new members with expertise in particular fields, like LOAC or diplomatic facilities, to take a first cut at their respective chapters. It would likely retain the methodology of the first process, as well as the original set of rules. And then the group as a whole—including that original group of human rights experts—would vote on the new provisions, edit them, determine how best to fit them into the rest of the manual, and perhaps add caveats so that the new chapters in Berlin 2.0 would not undermine the first set of rules they had laid out in Berlin 1.0. I think there is no question that such a process—even assuming the second manual were intended to cover precisely the same body of material as *Tallinn 2.0*, and even were the second group of experts comprising our alternate-universe Berlin 2.0 to be precisely the same people as those who were actually in the room during *Tallinn 2.0*—would yield a very different result.

B. Interpretation Catalysts at Stage Two

The second level at which the interpretation catalyst operates here is the *Tallinn* process itself as an impetus for states to develop cyber law in one particular field. One consistent refrain—in the *Tallinn Manual* itself and from the experts speaking on its behalf—is that the *Manual* is intended to represent the *lex lata* as it stood when the project was drafted and that the drafters did not see it as part of their mandate to push the law in a particular direction.[66] Yet the directors of the project have repeatedly stated their intent to impel states forward in clarifying the law in this space.[67] Moreover, for the reasons I laid out at the start of this section, and in more detail in

65. *See* PoKempner, *supra* note 22, at 1604 (discussing the myriad state, nonstate, and intergovernmental bodies and mechanisms involved in the interpretation and protection of human rights obligations).

66. *See, e.g.*, TALLINN MANUAL 2.0, *supra* note 5, at 3 ("*Tallinn Manual 2.0* is intended as an objective restatement of the *lex lata*. Therefore, the Experts involved in both projects assiduously avoided including statements reflecting *lex ferenda*."); *see also* Schmitt, *supra* note 3; Schmitt & Vihul, *supra* note 34.

67. *See, e.g.*, Schmitt, *supra* note 13 (describing one of *Tallinn 2.0*'s goals as "allow[ing] states to focus their efforts where clarification of the law is needed").

Interpretation Catalysts,[68] the simple existence of such a project, the path of its development, and the reality of its success in drawing the attention of states,[69] has already and will continue to act as a trigger influencing states in their own internal and group decision-making processes. That influence affects state decision making even at an incubatory stage, in the simple act of deciding whether to send an envoy to engage the *Tallinn* process, which specific official to send, from which agency component inside the government, and with what kind of expertise, and in the packaging of talking points the state puts together for that expert to deliver. The original *Tallinn* process's focus on the laws of war is inextricably intertwined with a concomitant need for states to engage with that process through their own law-of-war experts and resources. Should states then drive the law forward in the cyberwarfare realm, the experts leading the *Tallinn 1.0* process would rightfully mark that legal development a success, but we cannot ignore that this development must occur at the opportunity cost of a focus on other bodies of law that might subsequently be left less defined in the cyber realm.

C. *Harnessing the Power of Interpretation Catalysts*

This case study illustrates not only the power of interpretation catalysts in driving the direction of law as it develops, but also how such triggers can be harnessed, even manipulated, as a means of influencing the path that development takes. As I have noted, the initial Estonia cyber attacks, and the response to them, need not have been conceived primarily in war terms. In fact, the *Tallinn Manual* itself ultimately concluded both that "the law of armed conflict did not apply to those cyber operations because the situation did not rise to the level of an armed conflict," and that "there is no definitive evidence that the hacktivists involved in the cyber operations against Estonia in 2007 operated pursuant to instructions from any State, nor did any State endorse and adopt the conduct."[70] The resulting *Tallinn* project itself might thus have focused primarily on nonwartime legal questions, such as the prohibition on intervention, and indeed, on human rights law. Yet, as I noted above, there were incentives for state actors seeking to create this process to conceive of those events in war terms,[71] and that conception, in turn, may have enabled greater interest from state allies and prompted NATO engagement. In any event, whatever the impetus for that conception, these attacks, the atmospherics and language of "warfare" that surrounded them,

68. Ingber, *supra* note 3, at 360.

69. *See* Schmitt, *supra* note 13 (discussing "The Hague Process"); *Over 50 States Consult Tallinn Manual 2.0*, NATO COOP. CYBER DEF. CTR. OF EXCELLENCE (Feb. 2, 2017), https://ccdcoe.org/over-50-states-consult-tallinn-manual-20.html [https://perma.cc/3QKS-W3Y7].

70. TALLINN MANUAL 2.0, *supra* note 5, at 376, 382.

71. *See id.* at xxiii (stating, in an introductory note by the current President of Estonia, that the 2007 cyberattacks against Estonia marked "the first time one could apply the Clausewitzean dictum: War is the continuation of policy by other means").

the concomitant establishment of the NATO Cooperative Cyber Defence Centre of Excellence, and its immediate commissioning of the *Tallinn* study on cyber warfare, all determined the subsequent path for the development of the law in this space.

Conclusion

Doctrinal debates about the appropriate legal rules to apply to novel contexts at times mask institutional undercurrents that led to the adoption or interpretation of any particular rule. The initial triggers for the development of a legal position, and the institutional reality of the decision-making process that plays out, may have an enormous influence on the path that process takes and the resulting decision. Yet debates about doctrine do not typically address these triggers or the institutional process taken as a result.[72]

In concluding, it is worth considering some of the benefits inherent in a soft law process initially driven by law-of-war expertise and discipline. There is inherent in law-of-war-driven processes a focus on practical, operational rules and on how to employ them. There is a focus on states and what states will be willing to accept and implement, as well as useful—and to some degree unique—levels of engagement between scholars and practitioners working in this realm. The combination of practicality and engagement gives these experts added legitimacy in seeking to constrain state actors. And finally, at the broadest level, law-of-war experts are a group of individuals who have cut their teeth applying laws to space that others tend to see as lawless. That willingness to regulate what others may view as ungovernable is particularly important for an endeavor seeking to determine the rules applicable in cyberspace.

Considerations of institutions, actors, and process are critical when grappling with the development of law, and they are necessary to our consideration of the differing substantive bodies of law addressed in the *Tallinn Manual 2.0*. As the *Manual*'s directors have acknowledged, the discussion of human rights was a significant challenge for this project.[73] It has met with some criticism, and it may very well meet with more, particularly the more states rely upon it.[74] Debate will likely center on the specifics of the doctrinal rules, how the *Manual* grapples with those rules,

---

72. For a compelling account of how the evolution of the EU's human rights engagement turned on early, "pragmatic" decisions of the founding Member States, see Grainne De Burca, *The Road Not Taken: The EU as a Global Human Rights Actor*, 105 AM. J. INT'L L. 649 (2011).

73. *See* TALLINN MANUAL 2.0, *supra* note 5, at 4 (acknowledging the *Manual*'s limitation in the field of human rights law); Schmitt, *supra* note 13; *Tallinn Manual 2.0 to Be Completed in 2016*, NATO COOP. CYBER DEF. CTR. EXCELLENCE (Oct. 9, 2015), https://ccdcoe.org/tallinn-manual-20-be-completed-2016.html [https://perma.cc/VER5-QW7T] (quoting managing editor Liis Vihul as stating, "During this session, the most difficult material proved to be international human rights law governing activities in cyberspace.").

74. *See, e.g.*, *supra* Part I; PoKempner, *supra* note 22, at 1599.

and the difficulties in deriving clear legal guidance for states in this realm. But when considering those critiques, and the extent to which the *Manual* does or does not sufficiently drill down into any particular body of law, it is essential to contemplate the origins and path of the development of this project. The status of cyberlaw as it exists today is, and will continue to be, inextricably bound up in the initial approach taken to the events that triggered its development.

A Cyber Duty of Due Diligence: Gentle Civilizer or Crude Destabilizer?

Eric Talbot Jensen* and Sean Watts**

I. Introduction

In the final book of Virgil's epic poem the *Aeneid*, Latinus, King of Laurentum, delivers a speech to calm his aspirant son-in-law Turnus. Turnus is enraged that his rival Aeneas, cousin to the *Iliad*'s Hector, will marry the King's daughter instead. Turnus vows one-on-one combat with Aeneas to avenge the slight and to settle the war between the Trojans and Latins. King Latinus attempts to convince him not to fight Aeneas, imploring the prideful Turnus:

> Take to heart
> This fact: it was not right that I should pledge
> My daughter to a suitor of other days:
> Gods, and prophecies of men, forbade.
> Affection for you, our Rutulian kinsman,
> Won me over—and my wife in tears.
> I broke my bonds of duty, stole the girl,
> Though promised, from her husband, and took arms
> Against the will of heaven. You see what followed,
> Turnus: the bloody wars and the defeats,
> The bitter days you, most of all, endure.[1]

However, rather than calm Turnus, King Latinus's words aggravate him and propel him to fight Aeneas. Virgil describes the effect of the King's speech:

> All that he said affected Turnus's fury
> Not in the least: it mounted, all the more
> Fevered at words of healing.[2]

Virgil's original Latin captures the speech's effect with the phrase *aegrescit medendo*—the disease worsens with treatment or the cure worsens

---

* Professor, Brigham Young University Law School.

** Professor, Creighton University School of Law; Lieutenant Colonel, United States Army Reserve. The authors are grateful to Lt. Col. Theodore Richard for reviewing a draft of this article.

1. VIRGIL, THE AENEID, bk. XII, ll. 37–47, at 368 (Robert Fitzgerald trans., Vintage Books 2d. ed. 1985) (19 B.C.) [hereinafter THE AENEID].

2. *Id.* ll. 64–66, at 369.

the disease.[3] The lesson endures as a cautionary tale to well-meaning assistance to intractable predicaments.

The predicament of malicious cyber actions is by now well-documented. Harmful cyber activities range from embarrassment of public figures[4] and campaigns to build personal notoriety,[5] to thefts of personal data[6] and even efforts to cripple vital infrastructure upon which lives depend.[7] In financial terms, it is estimated that cybercrime costs the average U.S. company $15 million a year.[8] The problem, of course, is not limited to personal and business relations. Intrusive and malicious cyber operations are now a regular feature of international relations.[9] Cyber operations are thought to have struck at the core of some States' sovereignty, including the political processes of self-determination.[10]

---

3. THE WORKS OF P. VIRGILIUS MARO 349–50 (Levi Hart & V. R. Osborn trans., 1952).

4. Benjamin Weiser, *Man Who Hacked Celebrities' Email Accounts Gets 5 Years in Prison*, N.Y. TIMES (Dec. 6, 2016), https://www.nytimes.com/2016/12/06/nyregion/alonzo-knowles-celebrity-hacker.html [https://perma.cc/6DLX-DDLL].

5. Sooraj Shah, *Sony Facing Huge Challenge to Keep Secure as Hackers Seek Notoriety*, COMPUTING (Dec. 9, 2014), http://www.computing.co.uk/ctg/news/2385791/sony-facing-huge-challenge-to-keep-secure-as-hackers-seek-notoriety-says-sony-music-head-of-digital [https://perma.cc/AJ3P-9ZPJ].

6. Robert McMillan et al., *Yahoo Discloses New Breach of 1 Billion User Accounts*, WALL ST. J. (Dec. 15, 2016), https://www.wsj.com/articles/yahoo-discloses-new-breach-of-1-billion-user-accounts-1481753131 [https://perma.cc/NH3E-7Y8X].

7. Kim Zetter, *Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid*, WIRED (Mar. 3, 2016), https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/ [https://perma.cc/9W2U-5DGM].

8. James Griffiths, *Cybercrime Costs the Average U.S. Firm $15 Million a Year*, CNN TECH (Oct. 8, 2015), http://money.cnn.com/2015/10/08/technology/cybercrime-cost-business/ [https://perma.cc/NB3M-WX5F].

9. *See, e.g.*, Eric Beech & Ben Blanchard, *U.S., Chinese Officials Meet on Cyber Security Issues: White House*, REUTERS (Sept. 12, 2015), http://www.reuters.com/article/us-usa-china-cybersecurity-idUSKCN0RC0S420150913?feedType=RSS&feedName=internetNews [https://perma.cc/5MPM-DADF] (reporting on meetings of representatives from the United States and China to discuss cybersecurity and other issues); *Developments in the Field of Information and Telecommunications in the Context of International Security*, UNITED NATIONS OFF. FOR DISARMAMENT AFF. (Mar. 15, 2017), https://www.un.org/disarmament/topics/informationsecurity [https://perma.cc/F4H9-XLP5] (collecting submissions of global developments in cybersecurity); *NATO Holds Annual Cyber Exercise in Estonia*, NATO (Dec. 2, 2016), http://www.nato.int/cps/en/natohq/news_138674.htm [https://perma.cc/B3KG-NC9J] (discussing NATO's Cyber Coalition 2016, a three-day event where participants were tested and trained in cyber defense).

10. Oren Dorell, *Russia Engineered Election Hacks and Meddling in Europe*, USA TODAY (Jan. 9, 2017), http://www.usatoday.com/story/news/world/2017/01/09/russia-engineered-election-hacks-europe/96216556/ [https://perma.cc/4YC8-B6W2] (reporting examples of alleged Russian efforts to influence European election results through the use of cyber attacks); David E. Sanger & Scott Shane, *Russian Hackers Acted to Aid Trump in Election, U.S. Says*, N.Y. TIMES (Dec. 9, 2016), https://www.nytimes.com/2016/12/09/us/obama-russia-election-hack.html [https://perma.cc/M3KM-ZDZP] (reporting the "high confidence" of American intelligence agencies that Russia acted to influence the presidential election in Donald Trump's favor).

Responses have been many and varied. Governments have passed domestic legislation,[11] generated international agreements,[12] and convened groups of experts[13] to address the cyber predicament. Corporations have lobbied for (but have also resisted) new laws,[14] created and proposed information-sharing entities and norms,[15] and built capacity to respond in like manner to cyber hacks.[16] Meanwhile, academics and jurists have banded together to propose rules and produce manuals such as the *Tallinn Manuals*,[17] the second version of which is the genesis of this symposium.

Even when States are able to achieve either domestic or international consensus to counter harm in cyberspace, technical and legal limitations hinder progress. In particular, the dilemma of attribution, correctly identifying and holding responsible harmful actors, hampers many efforts. The nature of the Internet, including how it is configured and functions,

---

11. *See, e.g.*, Cybersecurity Act of 2015, Pub. L. No. 114–113, 129 Stat. 2244 (codified in scattered sections of 6 U.S.C.); Cory Bennett, *Congress Approves First Major Cyber Bill in Years*, THE HILL (Dec. 18, 2015), http://thehill.com/policy/cybersecurity/263696-congress-approves-first-major-cyber-bill-in-years [https://perma.cc/3KAX-88DV] (noting that the Cybersecurity Act of 2015 incentivizes companies to provide the government with data on hacking threats while providing protection against consumer lawsuits).

12. *See, e.g.*, Convention on Cybercrime, Nov. 3, 2001, S. TREATY DOC. No. 108–11, ETS No. 185 (reflecting coordinated efforts between European nations to combat cybercrime). China and Russia proposed a cyber code of conduct in 2011 and again in 2015. Letter dated 12 September 2011 from the Permanent Representatives of China, the Russ. Fed'n, Taj., and Uzb. to the U.N. Secretary-General, at 3–5, U.N. Doc. A/66/359 (Sept. 14, 2011); Letter dated 9 January 2015 from the Permanent Representatives of China, Kaz., Kyrg., the Russ. Fed'n, Taj., and Uzb. to the U.N. Secretary-General, U.N. Doc. 69/723 (Jan. 13, 2015).

13. U.N. Secretary-General, *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/70/174 (July 22, 2015) [hereinafter U.N. GGE Report 2015]; U.N. Secretary-General, *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) [hereinafter U.N. GGE Report 2013].

14. *See* Eric Engleman & Jonathan D. Salant, *Cybersecurity Lobby Surges as Congress Considers New Laws*, BLOOMBERG TECHNOLOGY (Mar. 21, 2013), https://www.bloomberg.com/news/articles/2013-03-21/cybersecurity-lobby-surges-as-congress-considers-new-laws [https://perma.cc/JM7U-TXU2?type=image] (reporting increased corporate lobbying in cybersecurity matters).

15. *See* Scott Charney et al., *From Articulation to Implementation: Enabling Progress on Cybersecurity Norms*, MICROSOFT (June 2016), https://mscorpmedia.azureedge.net/mscorpmedia/2016/06/Microsoft-Cybersecurity-Norms_vFinal.pdf [https://perma.cc/XS2Y-U2VQ] (discussing organizing models for cybersecurity norm development); Angela McKay et al., *International Cybersecurity Norms: Reducing Conflict in an Internet-Dependent World*, MICROSOFT (2014), aka.ms/cybernorms [https://perma.cc/6RKS-836V] (emphasizing the importance of norms in managing cybersecurity risks).

16. *See* Scott Cohn, *Companies Battle Cyberattacks Using 'Hack Back'*, CNBC (June 4, 2013), http://www.cnbc.com/id/100788881 [https://perma.cc/3G7M-LPRH] (discussing corporate efforts to hack cybercriminals in order to delete or alter stolen information).

17. TALLINN MANUAL 2.0 ON INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS (Michael N. Schmitt & Liis Vihul eds., 2017) [hereinafter TALLINN MANUAL 2.0]; TALLINN MANUAL ON INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE (Michael N. Schmitt ed., 2012).

makes attribution one of the most technically difficult and persistent impediments to preventing or mitigating cyber harm.[18] In cyberspace, anonymity is easily achieved and maintained not only in a personal sense, obscuring the identity of the person making keystrokes and clicks, but also in a technical sense, obscuring the location and identity of the cyber infrastructure from which harm originates.

A potential solution to the problem of attribution is a response proxy—an entity against whom action is taken when action against a responsible party is not feasible. The proxy system addressed in this Article is imbedded in the international law notion of State responsibility for transboundary harm. As will be explained below, holding a State responsible for allowing harmful activities to emanate from its territory that produce significant effects on another State is increasingly supported by international law. Recognizing a cyber-specific obligation of due diligence to address emanation of such cyber harms might mitigate the attribution dilemma. That is, a primary rule of conduct requiring diligent management of territorial cyber infrastructure could give rise to responsibility on the part of nondiligent States as proxies for unidentified or unreachable malicious actors. Legal recognition of such breaches of diligence permits State victims of cyber harm to take action to induce compliance and terminate harm without necessarily tracing attribution to the original, difficult-to-identify source. Such an approach has gained momentum among both States[19] and commentators.[20]

However, on examination, proxy responses by way of a cyber duty of due diligence may actually be, if aggressively applied, counterproductive and lead to greater instability in the international system. Although development of primary rules of conduct in international law is generally thought to increase stability and cooperation, recognition and refinement of a duty of cyber due diligence might impose significant costs to security, stability, and even to international law compliance. In this Article, an outline of the principles of State responsibility illustrates how international law generally holds States accountable for and manages their responses to legal breaches and harm. A portrayal of the doctrine of countermeasures, a longstanding international law response to illegal acts by another State, highlights one of the most important self-help remedies of State responsibility. Analysis of the principle of due diligence in cyberspace and its relationship to

18. Thomas Rid & Ben Buchanan, *Attributing Cyber Attacks*, 38 J. STRATEGIC STUD. 4, 5 (2015).

19. *See* U.N. GGE Report 2015, *supra* note 13, at 7–8 (reaffirming that States should promote cybersecurity and take actions that consider the challenges of attribution); U.N. GGE Report 2013, *supra* note 13, at 8 (establishing the principle that States should ensure that their territories are not used for cyber attacks and recognizing the challenges of attribution).

20. Scott Shackelford et al., *Unpacking the International Law on Cybersecurity Due Diligence: Lessons from the Public and Private Sectors*, 17 CHI. J. INT'L L. 1, 19 (2016) (arguing that a State's failure regarding due diligence may empower victim States to respond with cyber countermeasures).

countermeasures illustrates an initially attractive solution to the attribution dilemma. But a concluding cautionary note identifies potential unintended consequences of due diligence-inspired countermeasures as an attempt to close the attribution gap. Ultimately, due diligence could be an effective tool in justifying the use of countermeasures in the fight against the difficulties caused by the inability to attribute harmful cyber acts—but, like King Latinus's speech, the cure may worsen the disease.

II. State Responsibility and Attribution

States often evade responsibility for their transnational cyber activities. The Stuxnet worm is rumored to have been the unclaimed work of the United States and Israel.[21] Russia allegedly conducted a cyber operation to shut down power-generation facilities in Ukraine.[22] The United States has accused North Korea of hacking Sony Pictures information systems and communications.[23] And in 2014, the United States indicted five members of the Chinese People's Liberation Army for alleged hacking into U.S. systems.[24] In none of these cases, and in none of the many others like them, did the supposed "hacking" State admit commission, complicity, or responsibility.[25]

The legal notion of State responsibility dates to recognition of the State as the focal point of the international legal system. The State's monopoly on power within its borders supported the conclusion that external uses of State power were attributable to the State itself.[26] Over time, State responsibility

---

21. *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 [https://perma.cc/NH6T-U9G9] (stating that joint American–Israeli operations out of a complex in the Negev Desert "are among the newest and strongest clues suggesting that the virus was designed as an American–Israeli project to sabotage the Iranian program").

22. Zetter, *supra* note 7.

23. *See, e.g.*, Alex Altman & Zeke J. Miller, *FBI Accuses North Korea in Sony Hack*, TIME (Dec. 19, 2014), http://time.com/3642161/sony-hack-north-korea-the-interview-fbi/ [https://perma.cc/5GTG-728U] (describing how the FBI accused the North Korean government of being involved in the Sony Pictures hack); Andrea Peterson, *The Sony Pictures Hack, Explained*, WASH. POST (Dec. 18, 2014), https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained/?utm_term=.6cd248ebbcab [https://perma.cc/M48M-HBV9] (explaining the Sony hacks and how U.S. government agencies believe that North Korea was responsible).

24. Gina Chon, *US Pursues Case Against Chinese Army Hackers*, FIN. TIMES (Sept. 24, 2015), https://www.ft.com/content/a378b4c6-62b0-11e5-9846-de406ccb37f2 [https://perma.cc/BU5W-GNHW].

25. *See, e.g.*, Ellen Nakashima, *Indictment of PLA Hackers is Part of Broad U.S. Strategy to Curb Chinese Cyberspying*, WASH. POST (May 22, 2014), https://www.washingtonpost.com/world/national-security/indictment-of-pla-hackers-is-part-of-broad-us-strategy-to-curb-chinese-cyberspying/2014/05/22/a66cf26a-e1b4-11e3-9743-bb9b59cde7b9_story.html?utm_term=.391e8d6d33b4 [https://perma.cc/2LXX-4VZN] (noting that the Chinese government denied any connection to hacking by PLA agents).

26. *See* PHILIP BOBBITT, THE SHIELD OF ACHILLES: WAR, PEACE AND THE COURSE OF HISTORY 80–90, 96–118 (2002) (recounting the Renaissance-era consolidation of power from

doctrine deepened in its complexity and reach.[27] In 2001, after nearly four decades of work, the United Nations International Law Commission (ILC) adopted and submitted its Draft Articles on Responsibility of States for Internationally Wrongful Acts.[28] The United Nations General Assembly has since commended them to its member States.[29] States have lodged few substantial objections to the substance of the Articles,[30] suggesting they may, in great part, reflect customary international law. The *Tallinn Manual 2.0* acknowledges the validity of the ILC Articles and relies heavily on them to describe existing rules on State responsibility.[31]

The widely accepted formula for State responsibility, echoed in the ILC Articles, is: (1) a breach of an international obligation and (2) attribution to a State under international law.[32] To establish State responsibility, an act must not only be harmful, it must also amount to a breach of the offending State's international legal obligations.[33] Qualifying breaches may be either in the nature of an act or omission.[34] Further, the fact that a harmful cyber activity originates from within a State's territory does not necessarily mean that the State is responsible. For responsibility to accrue to the State, the act must be attributable to the State, either as an act of "its organs of government, or of others who have acted under the direction, instigation or control of those organs, i.e. as agents of the State."[35]

---

princedoms to absolutist "kingly states"); Frederic Gilles Sourgens, *Positivism, Humanism, and Hegemony: Sovereignty and Security for Our Time*, 25 PA. ST. INT'L L. REV. 433, 443 (2006) (citing sixteenth-century writer Bodin as defining sovereignty as the "absolute and perpetual power of the commonwealth resting in the hands of the state").

27. *See* James Crawford, *Articles on Responsibility of States for Internationally Wrongful Acts*, U.N. AUDIOVISUAL LIBR. OF INT'L L. 1–2 (2012), http://legal.un.org/avl/pdf/ha/rsiwa/rsiwa_e.pdf [https://perma.cc/A2U5-WST2] (discussing the history and development of the articles).

28. Int'l L. Comm'n, Draft Articles on Responsibility of States for Internationally Wrongful Acts, U.N. Doc. A/56/10 (2001) [hereinafter Articles of State Responsibility]; Int'l L. Comm'n, Draft Articles on Responsibility of States for Internationally Wrongful Acts with Commentaries (2001), http://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf [https://perma.cc/96QH-EJ6Z] [hereinafter ASR Commentaries].

29. G.A. Res. 56/83, ¶ 3 (Jan. 28, 2002); G.A. Res. 59/35, ¶ 1 (Dec. 16, 2004).

30. *See, e.g.*, U.S. Dep't of State, Draft Articles on State Responsibility: Comments of the Government of the United States of America (1997), https://www.state.gov/documents/organization/65781.pdf [https://perma.cc/82HM-3JA6] (detailing the United States' objections to the Articles of State Responsibility where the United States believed certain provisions were not in accord with international law).

31. TALLINN MANUAL 2.0, *supra* note 17, at 79.

32. Articles of State Responsibility, *supra* note 28, art. 2.

33. ASR Commentaries, *supra* note 28, at 35; TALLINN MANUAL 2.0, *supra* note 17, at 85–86.

34. Articles of State Responsibility, *supra* note 28, art. 2; ASR Commentaries, *supra* note 28, at 35. For more on this topic, see Franck Latty, *Acts and Omissions*, *in* THE LAW OF INTERNATIONAL RESPONSIBILITY 355, 355 (James Crawford et al. eds., 2010).

35. ASR Commentaries, *supra* note 28, at 38.

Attribution attaches most clearly when an organ of a State conducts an act itself.[36] An organ of the State includes "any person or entity which has that status in accordance with the internal law of the State."[37] In the United States, this would include government entities such as the Department of Defense and its Cyber Command and National Security Agency, as well as the Central Intelligence Agency and Secret Service.[38] Responsibility for acts of State organs even extends to *ultra vires* acts.[39] The International Court of Justice has observed, "[P]ersons, groups of persons or entities [may be responsible] . . . even if that status does not follow from internal law, provided that in fact the persons, groups or entities act in 'complete dependence' on the State, of which they are ultimately merely the instrument."[40]

Acts by persons or entities exercising elements of governmental authority are also attributable to States.[41] However, attribution by such means only arises when the persons or entities are "acting in that capacity in the particular instance."[42] Such entities might include:

> public corporations, semipublic entities, public agencies of various kinds and even, in special cases, private companies, provided that in each case the entity is empowered by the law of the State to exercise functions of a public character normally exercised by State organs, and the conduct of the entity relates to the exercise of the governmental authority concerned.[43]

An example of such an entity might be a private company employed by a State, with appropriate regulatory authority, to defend State networks.[44]

Attribution to a State can also be established through acts by organs of another State placed at the disposal of the offending State, so long as the acting organ is exercising elements of authority of the offending State.[45] To meet this criterion, the organ must "act in conjunction with the machinery of

---

36. Articles of State Responsibility, *supra* note 28, art. 4; TALLINN MANUAL 2.0, *supra* note 17, at 87.

37. Articles of State Responsibility, *supra* note 28, art. 4.2.

38. *See, e.g.*, TALLINN MANUAL 2.0, *supra* note 17, at 87 (recognizing the United States' Cyber Command as a State organ); Articles of State Responsibility, *supra* note 28, art. 4 (defining conduct of organs of a State).

39. Articles of State Responsibility, *supra* note 28, art. 7.

40. Application of Convention on Prevention and Punishment of Crime of Genocide (Bosn. & Herz. v. Serb. & Montenegro), 2007 I.C.J. Rep. 43, ¶ 392 (Feb. 26).

41. Articles of State Responsibility, *supra* note 28, art. 5; TALLINN MANUAL 2.0, *supra* note 17, at 89.

42. TALLINN MANUAL 2.0, *supra* note 17, at 89.

43. ASR Commentaries, *supra* note 28, at 43; *see also* TALLINN MANUAL 2.0, *supra* note 17, at 89 (providing examples of private entities empowered by domestic law to conduct cybersecurity or intelligence operations).

44. TALLINN MANUAL 2.0, *supra* note 17, at 90.

45. Articles of State Responsibility, *supra* note 28, art. 6; TALLINN MANUAL 2.0, *supra* note 17, at 93 (Rule 16).

that State and under its exclusive direction and control, rather than on instructions from the sending State."[46] The organ cannot be serving "the purposes of the former State or even . . . shared purposes" under this method of attribution.[47] So, for example, if a State loaned its Computer Emergency Readiness Team (CERT) to another State to assist with a cyber activity, but required the CERT to get permission for any action that might have transboundary effects, the action of the CERT would not be attributable to the receiving State under this theory.[48]

A final method of State attribution is through acts by persons or groups acting on the instructions of a State or under its direction or control.[49] The ILC Articles describe situations where "State organs supplement their own action by recruiting or instigating private persons or groups who act as 'auxiliaries'" as well as situations where the conduct by non-State actors was "directed or controlled" by the State and "an integral part of that operation."[50] The International Court of Justice (ICJ) has determined that control necessary for attribution of a non-State actor's actions to the State is exercise of "effective control" by the latter.[51] Thus, if a private hacking group conducted malicious cyber activity against another State specifically under the instructions of a State agency or if the State agency exercised effective control of those actions, the act would be attributable to the State.

The principal significance of State responsibility is international accountability. In international law circles, State responsibility is often envisioned to attach for purposes of litigation. Subject to jurisdictional requirements, a responsible State can expect to be ordered to cease its conduct and to provide a remedy to a victim State. But State responsibility can be important outside litigation as well. State responsibility may be valuable legal capital in diplomatic negotiations. More significant perhaps, State responsibility can give a victim State the opportunity to respond to the transgressing State's actions, including resort to countermeasures.

---

46. ASR Commentaries, *supra* note 28, at 44; *see also* TALLINN MANUAL 2.0, *supra* note 17, at 93 (clarifying that "if the organ continues to receive any instructions as to its operations from the sending State," then the actions of the organ are not attributable to the receiving State).

47. ASR Commentaries, *supra* note 28, at 44.

48. TALLINN MANUAL 2.0, *supra* note 17, at 93–94.

49. Articles of State Responsibility, *supra* note 28, art. 8.

50. ASR Commentaries, *supra* note 28, at 47.

51. Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. Rep. 14, ¶ 115 (June 27); *see also* ASR Commentaries, *supra* note 28, at 47–48 (identifying circumstances in which personal or group actions are considered State actions); TALLINN MANUAL 2.0, *supra* note 17, at 96–97 (indicating under which conditions cyber operations will be attributed to States even when committed by non-State actors).

III. Countermeasures

Countermeasures are otherwise unlawful State acts that are lawful when undertaken to induce another State to cease unlawful conduct against it.[52] Given the decentralized, self-governing nature of international law, countermeasures are an important form of international law self-help.[53] The modern conception of countermeasures grew out of the traditional concept of reprisals and now replaces the traditional concept of nonforceful reprisals that occur outside of armed conflict.[54] They are distinct from acts of retorsion—unfriendly but lawful acts—and would be otherwise unlawful.[55]

Because of their potential to undermine international law, countermeasures are subject to important restrictions.[56] First, countermeasures may only be undertaken to induce compliance by a State in breach of international law.[57] Countermeasures may not be undertaken to punish.[58] An important corollary to this restriction, likely a vestige of the State-centric international legal system, is that countermeasures must be directed at another State and may not be undertaken against non-State actors that operate independently from a State.[59] A countermeasure need not, however, involve or be directly linked to the same or any related obligation the offending State breached.[60]

---

52. *See* Gabčikovo-Nagymaros Project (Hung. v. Slovk.), Judgment, 1997 I.C.J. Rep. 7, ¶¶ 82–83 (Sept. 25) (discussing the requirements for lawful countermeasures); *see also* ASR Commentaries, *supra* note 28, at 128 (commenting that countermeasures must be taken in response to unlawful international acts); Michael N. Schmitt, *"Below the Threshold" Cyber Operations: The Countermeasures Response Option and International Law*, 54 VA. J. INT'L L. 697, 700 (2014) (defining countermeasures along similar lines).

53. *See* ASR Commentaries, *supra* note 28, at 128 (observing that countermeasures are an aspect of a decentralized international system that allows States to vindicate their rights when harmed by internationally wrongful acts).

54. *See id.* (describing and defining "reprisals").

55. *Id.*; *see* Schmitt, *supra* note 52, at 701–02 (distinguishing retorsion from countermeasures).

56. ASR Commentaries, *supra* note 28, at 128.

57. Articles of State Responsibility, *supra* note 28, art. 49; *see also* ASR Commentaries, *supra* note 28, at 130 (explaining that an internationally wrongful act is a "fundamental prerequisite" for any lawful countermeasure).

58. ASR Commentaries, *supra* note 28, at 130.

59. *See* Articles of State Responsibility, *supra* note 28, art. 49 (limiting the object of countermeasures to a State responsible for an internationally wrongful act); *see also* ASR Commentaries, *supra* note 28, at 129–30 (analyzing limitations on countermeasures undertaken by injured States).

60. ASR Commentaries, *supra* note 28, at 129. But note, "[c]ountermeasures are more likely to satisfy the requirements of necessity and proportionality if they are taken in relation to the same or a closely related obligation . . . ." *Id.*

Second, only a victim State may resort to countermeasures.[61] Third-party States may not undertake countermeasures on behalf of another State.[62] Third, countermeasures may not rise to the level of force.[63] Use of force by States is restricted to self-defense and actions authorized by the United Nations Security Council.[64] Fourth, countermeasures must be necessary and proportionate to the international wrong that provokes them.[65] Fifth, countermeasures should be temporary and reversible, so when the international wrong ceases, the countermeasures also cease and their effects are reversed.[66] And finally, countermeasures must be preceded by a demand to cease the unlawful activity that gives rise to their use.[67]

Thus, a State that suffers cyber harm from an internationally wrongful act by another State may resort to countermeasures when that act is attributable, through any of the various forms of liability, to another State. Or at least that is the case in theory. While wrongfulness may be easily established, as mentioned above, attribution is notoriously elusive and difficult in cyberspace. Cyber means offer actors any number of techniques to mask their identities, to spoof others' identities, or to otherwise mislead or frustrate victims' efforts at establishing accountability. A State that suffers harm by cyber means but is unable to establish attribution to another State has not affixed State responsibility, and therefore may not undertake countermeasures. In this sense, the victim State might be said to face an attribution-response gap.

IV. Due Diligence and the Attribution-Response Gap

The difficulty of establishing attribution sufficient to give rise to responsibility greatly complicates efforts to respond with anything more than measures of retorsion such as sanctions or public diplomatic protests. Without attribution, countermeasures are unavailable or, at minimum, extraordinarily risky. Although international law does not prescribe a

---

61. Articles of State Responsibility, *supra* note 28, arts. 49, 54; TALLINN MANUAL 2.0, *supra* note 17, at 130–33 (Rule 24).

62. *See* TALLINN MANUAL 2.0, *supra* note 17, at 132 (explaining that a majority of the Experts took the position that third-party countermeasures are unlawful).

63. *See* Articles of State Responsibility, *supra* note 28, art. 49 (requiring that a State's countermeasures be limited to nonperformance of international obligations).

64. *See* U.N. Charter arts. 2, 42, 51 (establishing that while States retain their inherent right to act in self-defense, they must refrain from other uses of force without Security Council approval).

65. Articles of State Responsibility, *supra* note 28, arts. 49, 51; TALLINN MANUAL 2.0, *supra* note 17, at 127 (Rule 23).

66. *See* Articles of State Responsibility, *supra* note 28, art. 49 (delimiting the acceptable breadth and methods of countermeasures); ASR Commentaries, *supra* note 28, at 129–31 (stressing that countermeasures should be temporary and reversible because their purpose is only to induce cessation of wrongdoing, not to punish).

67. Articles of State Responsibility, *supra* note 28, art. 52; ASR Commentaries, *supra* note 28, at 129.

prerequisite evidentiary burden with respect to undertaking countermeasures, a State is responsible for countermeasures that are later proved undertaken on the basis of flawed or mistaken evidence.[68] A State that is unable to establish attribution to a reliably certain level thus accepts the risk that its countermeasures will themselves amount to an internationally wrongful act.[69] Greater application of the doctrine of due diligence to cyber activities originating from States, however, may help bridge the attribution gap, making the use of countermeasures available to an aggrieved State. It is possible that increased breadth and clarity to the doctrine of due diligence would ease the ability of the target state to attribute the cyber activity to another State, thus enlarging the opportunity to use countermeasures.

A. Definition of Due Diligence

In part to address the attribution-response gap, recent enthusiasm has developed for the notion of an international obligation of cyber due diligence. The principle of due diligence is not new to international law and has roots in the ancient maxim *sic utero tuo ut alienum non laedas* (use your own property in such a manner as not to injure that of another).[70] More recently, a 1949 case decided by the ICJ described something very much like due diligence when it noted "every State's obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States."[71] Similarly, a 1941 international arbitral award between the United States and Canada observed, "no State has the right to use or permit the use of its territory . . . to cause injury . . . to the territory of another . . . when the case is of serious consequence."[72] The obligation to neither commit nor allow harm to emanate from a State's borders has been codified in numerous international agreements, particularly in the area of international environmental law.[73]

---

68. JAMES CRAWFORD, THE INTERNATIONAL LAW COMMISSION'S ARTICLES ON STATE RESPONSIBILITY: INTRODUCTION, TEXT AND COMMENTARIES 285 (2002).

69. ASR Commentaries, *supra* note 28, at 130; *see* TALLINN MANUAL 2.0, *supra* note 17, at 116 (suggesting that countermeasures may themselves constitute a wrongful act if taken against a State mistakenly attributed with cyber activities, but not actually responsible for them).

70. Jutta Brunnée, *Sic utero tuo ut alienum non laedas*, *in* 9 THE MAX PLANCK ENCYCLOPEDIA OF PUBLIC INTERNATIONAL LAW 188 (Rudiger Wolfram ed. 2012).

71. Corfu Channel (U.K. v. Alb.), Judgment, 1949 I.C.J. Rep. 4, at 22 (Apr. 9).

72. Trail Smelter (U.S. v. Can.), 3 R.I.A.A. 1905, 1965 (Trail Smelter Arb. Trib. 1941); *see also* TALLINN MANUAL 2.0, *supra* note 17, at 30–31 (describing the background duty of States to refrain from and control efforts to do harm to other States from within their territories).

73. *See* Convention on Biological Diversity art. 3, June 5, 1992, 1760 U.N.T.S. 79 (acknowledging the right of States to exploit their natural resources but also their duty not to cause damage to the environments of other States); United Nations Framework Convention on Climate Change art. 2, May 9, 1992, S. TREATY DOC. No. 102-38, 1771 U.N.T.S. 107 (recognizing the duty of States to refrain from causing harm to the natural environments of other States); Convention on Long-Range Transboundary Air Pollution art. 2, Nov. 13, 1979, T.I.A.S. 10541, 1302 U.N.T.S. 217 (agreeing to limit and reduce air pollution that emanates from one State and causes harm in another).

This duty of due diligence represents the "standard of conduct expected of States when complying with this principle."[74]

As a standard, due diligence requires a State to do that which is generally considered to be appropriate and proportional to the degree of risk of transboundary harm in the particular instance.[75] In other words, the requirement is one of reasonableness.[76] States cannot be expected to prevent every harm; the principle of *sic utere tuo ut alienum non laedas* assumes that victim States must accept some harm under the doctrine of good neighborliness.[77]

At present, several doctrinal ambiguities surround due diligence, but most of its proponents agree that the duty arises only with respect to known harm[78] and a State need only undertake reasonably feasible measures to cease offending uses of its territory.[79] Most also agree that there is no duty to affirmatively monitor networks or to prevent offending use of cyber infrastructure.[80] Additionally, though international law is unclear as to the precise level of harm required to trigger the due diligence obligation, it is generally accepted that the harm must amount to serious adverse consequences.[81]

B. The Application of Due Diligence to the Cyber Context

The *Tallinn Manual 2.0* concludes that the duty of due diligence applies in the cyber context. Chapter 2 of the *Manual* contains two rules and significant commentary to support this assertion. The first rule on due diligence, Rule 6, observes, "A State must exercise due diligence in not allowing its territory, or territory or cyber infrastructure under its governmental control, to be used for cyber operations that affect the rights of, and produce serious adverse consequences for, other States."[82] The commentary to Rule 6 clarifies that for the due diligence obligation to attach,

---

74. TALLINN MANUAL 2.0, *supra* note 17, at 30.

75. In the Alabama Arbitration of 1872 between the United States and the United Kingdom, due diligence was defined as "a failure to use for the prevention of an act which the government was bound to endeavour to prevent, such care as governments ordinarily employ in their domestic concerns, and may reasonably be expected to exert in matters of international interest and obligation." *Case Presented on the Part of the Government of Her Britannic Majesty to the Tribunal*, *in* PAPERS RELATING TO THE FOREIGN RELATIONS OF THE UNITED STATES 412 (1872); Timo Koivurova, *Due Diligence*, *in* 3 THE MAX PLANCK ENCYCLOPEDIA OF PUBLIC INTERNATIONAL LAW 242 (Rudiger Wolfrum ed., 2012).

76. Koivurova, *supra* note 75, at 236.

77. Brunnée, *supra* note 70, at 190.

78. *See* TALLINN MANUAL 2.0, *supra* note 17, at 40–43 (discussing the requirement of knowledge in exercising due diligence).

79. *Id.* at 43 (Rule 7).

80. *Id.* at 43–50.

81. *See id.* at 45 (explaining that a duty of prevention would place an "undue burden on States" and negate the Rule's knowledge requirement).

82. *Id.* at 30 (Rule 6).

a State must have knowledge (including constructive knowledge), and that the harm must rise to the level of serious adverse consequences.[83]

Rule 7 then states, "The principle of due diligence requires a State to take all measures that are feasible in the circumstances to put an end to cyber operations that affect a right of, and produce serious adverse consequences for, other States."[84] The commentary to Rule 7 emphasizes that the State is only required to take feasible measures in attempting to prevent the harm and that there is no duty to monitor cyber infrastructure in order to comply with the due diligence obligation.[85]

Despite any limitations that might apply to the due diligence principle in the cyber context, including those argued for by the International Group of Experts that wrote the *Tallinn Manual 2.0*, the application of the due diligence principle to cyber operations is an important application of international law to emerging technology. Applying due diligence to cyber operations also implicates the application of State responsibility and may have far-reaching impacts on how States respond to transboundary cyber activities.

C. Due Diligence as a Response Measure

Scholars have seized on due diligence as a promising way to ensure responsible and secure use of cyber infrastructure and to bolster peaceful and cooperative management of cyberspace by States.[86] A less appreciated advantage of applying due diligence to cyberspace, however, might be alleviation of the attribution-response gap noted above. Consider the following: State A suffers cyber incitements to violence conducted by State B, launched from or routed through cyber infrastructure on territory of State C. Suppose the violence is sufficient to coercively influence political events in State A. Suppose further that State A is unable to determine precisely who is responsible for the cyber incitements. State A is only able to discern that the cyber incitements emanated from infrastructure in State C. Under the law of State responsibility, although State A has suffered an internationally wrongful act, State A could not resort to countermeasures against either State B or State C because it cannot attribute the incitements. Recall that failure of attribution denies an attachment of State responsibility making countermeasures unavailable.

---

83. *Id.* at 36–37, 40–41.

84. *Id.* at 43 (Rule 7).

85. *See id.* at 43–46 (explaining that a general duty of prevention is not required, but a State's due diligence responsibility extends to preventing cyber operations when material steps to execute the operation have been carried out; however, this duty does not include a duty to monitor).

86. *See generally* Shackelford et al., *supra* note 20 (discussing the creation of cyber due diligence norms).

If, however, an obligation of cyber due diligence is recognized, as the territorial State, State C could be responsible for failing its duty to stop harm emanating from its territory. If State A informs State C early of the harm and State C, aware that its cyber infrastructure is being used to harm State A, does not terminate the cyber incitements, State C is in breach of its due diligence obligation. State C's breach of due diligence constitutes an independent internationally wrongful act and State A may, subject to the limitations mentioned previously, resort to countermeasures against State C. In this sense, the duty of due diligence mitigates against the response gap resulting from the failures of attribution so common in cyberspace.

V. Costs of the Due Diligence Approach

Recognition of a duty of due diligence in cyberspace is, of course, not without potential drawbacks. The countermeasures that become available to States in cases of breach of due diligence are important aspects of self-help in the international legal system. However, because they involve conduct in breach of international law, they may work subtly to undermine the international legal system and its goal of maintaining international peace and security if not carefully applied. Even after a victim State observes the considerable procedural safeguards and prerequisites attendant to lawful countermeasures (e.g., notice, a demand to cease, and proportionality),[87] considerable hazard is involved in their use. Concerns both theoretical and practical associated with countermeasures come to mind, including erosion of State internalization of international law, proliferation of resorts to self-help, hindrance of multilateral and collective capacity, and faulty assignments of culpability.

A. Rule Erosion

A first, significant concern arising from resorts to countermeasures is that they may condition States and their agents to think more cynically (or, if one prefers, realistically[88]) about international law. Explanations why States

87. *See supra* text accompanying notes 51–60.

88. *See, e.g.*, KENNETH N. WALTZ, THEORY OF INTERNATIONAL POLITICS 88–91 (1979) (noting the sphere of international politics suffers from lack of order and organization); *see also* HERSCH LAUTERPACHT, THE FUNCTION OF LAW IN THE INTERNATIONAL COMMUNITY 400 n.1 (1933) (tracing, though not supporting, a realist view of international law to Hobbes's *Leviathan*); HANS J. MORGENTHAU, POLITICS AMONG NATIONS: THE STRUGGLE FOR POWER AND PEACE 282 (4th ed. 1968) (arguing that a great power can act against a smaller power under the pretext of taking a countermeasure without fear or retribution from the smaller nation); Raymond Aron, *The Anarchical Order of Power*, *in* CONDITIONS OF WORLD ORDER 25, 26 (Stanley Hoffman ed., 1968) ("The society of states is by essence a-social, since it does not outlaw the recourse to force the 'collective persons' that are its members."); Hans J. Morgenthau, *Positivism, Functionalism, and International Law*, 32 AM. J. INT'L L. 260, 260–61 (1940) (referring to the lay view that there are large gaps between how international law works in theory and how it works out in practice as "realistic").

follow international law abound. Among many theories is the belief that States comply with international law because they internalize its rules of conduct.[89] There is legitimate theoretical concern that countermeasures may reverse norm internalization and therefore degrade States' compliance with international law.

International law constructivism, and the many variants thereof, observe that States obey international law most of the time and concludes that "[m]uch compliance can be attributed to institutionalized habit."[90] Constructivists explain that over time State organs and actors develop routine practices in their international decision making drawn from international rules and norms.[91] These practices and institutional habits are often drawn from courses of conduct prescribed by international instruments such as treaties.[92] Other institutional habits form from compliance with binding international custom.[93] Most of this internalization is thought to occur in domestic executive branch agencies—the bureaucrats and legal professionals who chiefly implement States' international legal policies.[94] However, rule internalization has been extensively documented in domestic courts.[95] Internalization has also been thought to operate at more fundamental and consequential levels. Dean Harold Koh has argued that international law plays a role in the formation of national identity.[96] Observed subconsciously or by default, the constructivist perspective, especially its more recent incarnation, asserts international rules become so ingrained "that possibilities of action contrary to the law do not even rise to conscious decision-making."[97]

---

89. *See* Harold Hongju Koh, *Why Do Nations Obey International Law?*, 106 YALE L.J. 2599, 2602 (1997) (examining schools of thought on international law and observing that global norms are "ultimately *internalized* by domestic legal systems"); *see also* Ryan Goodman & Derek Jinks, *Toward an Institutional Theory of Sovereignty*, 55 STAN. L. REV. 1749, 1752, 1785–86 (2003) (remarking that States tend to reflect and operate off "global scripts").

90. OSCAR SCHACHTER, INTERNATIONAL LAW IN THEORY AND PRACTICE 7 (1991).

91. *See* Koh, *supra* note 89, at 2634, 2646–57 (describing a three-step process in which international actors adopt international customs through interaction, interpretation, and internalization).

92. SCHACHTER, *supra* note 90, at 7.

93. *See id.* (explaining that most actors observe international law because the officials involved have internalized the rules and customs). *See generally* Edward M. Morgan, *Internalization of Customary International Law: An Historical Perspective*, 12 YALE J. INT'L L. 63 (1987) (discussing the historical development of the modern internalization doctrine).

94. *See* Amichai Cohen, *Bureaucratic Internalization: Domestic Governmental Agencies and the Legitimization of International Law*, 36 GEO. J. INT'L L. 1079, 1100–02 (2005) (discussing how executive branch officials converge on and craft policies consistent with international law).

95. *See* Harold Hongju Koh, *International Law as Part of Our Law*, 98 AM. J. INT'L L. 43, 44 (2004) (tracing internalization of international law to early U.S. Supreme Court decisions by Chief Justice John Marshall).

96. Koh, *supra* note 89, at 2655.

97. SCHACHTER, *supra* note 90, at 7.

If internalization occurs and if, as constructivists maintain, it conditions States to routine, subconscious compliance, one might expect resorts to countermeasures to reverse or at least compromise the phenomenon. At minimum, resorts to countermeasures cause compliance decisions to re-enter conscious thought. Once a State learns it has suffered an international wrong at the hands of another State and resolves to respond with self-help, a countermeasures calculus could be said to begin. Especially with respect to breaches of highly internalized norms, resort to countermeasures involves a deliberate reconsideration of previously rote compliance. The norm selected for breach as a countermeasure is likely to be evaluated methodically and perhaps even reconsidered entirely. In this sense, and because they involve undertaking conduct that would otherwise be internationally wrongful, countermeasures upset the "default patterns of compliance" described by Koh.[98]

The range of norms undermined by a countermeasures scenario could be exceptionally broad, far more broad than other means of self-help such as negative reciprocity or treaty suspension.[99] It is especially important to appreciate that countermeasures are distinct from negative reciprocity. Negative reciprocity involves rejection of a specific norm not observed or undertaken by another State.[100] Countermeasures need not involve breach of the same rule or norm that the offending State breached.[101] In fact, a countermeasure may involve a norm entirely unrelated to the rule involved in the underlying breach.[102] It is true that discourse on countermeasures includes in some cases a requirement of "relevance."[103] Yet in this case, relevance refers only to a logical connection between the breach selected and its propensity to draw the offending State into line with its legal obligations. The countermeasure selected must be relevant to a resumption of legal behavior and need only be selected for its propensity to induce the offending State back to compliance.

In this way, decisions involving countermeasures may lead a State to contemplate a far broader array of international norms than mere negative

98. Koh, *supra* note 89, at 2655.

99. *See* Vienna Convention on the Law of Treaties art. 60, May 23, 1969, 1155 U.N.T.S. 331 (providing for treaty termination or suspension in consequence of a material breach of a bilateral treaty).

100. *See* ELISABETH ZOLLER, PEACETIME UNILATERAL REMEDIES: AN ANALYSIS OF COUNTERMEASURES 20 (1984) (noting the backward-looking nature of negative reciprocity).

101. ASR Commentaries, *supra* note 28, at 129. The Commentaries observe, "There is no requirement that States taking countermeasures should be limited to suspension of performance of the same or a closely related obligation." *Id.*

102. *See id.*

103. *See* David J. Bederman, *Counterintuiting Countermeasures*, 96 AM. J. INT'L L. 817, 827 (2002) (noting that the proper role of relevance in countermeasures remains a matter of debate "that will need to be closely watched").

reciprocity.[104] To be sure, not all rules and norms are in play for countermeasures. Countermeasures may not involve breach of peremptory norms.[105] Constructivists might maintain that more deeply internalized international norms are less likely to be the means of countermeasures. Still, because countermeasures need not involve breach of an identical norm, the range of norms available for consideration is enormous, and the potential for reversals of internalization seems great.

Reversals of internalization occasioned by resorts to due diligence-minded countermeasures could occur on any number of levels. Although far from identifying with the constructivist theory, Kenneth Waltz identifies three levels at which international relations decisions, including international law compliance, can be analyzed: international, State, and individual or agency levels.[106] Just as international law can be internalized at any of these levels, countermeasures seem capable of undermining internalization at each of these levels of compliance. Breach of an international rule of conduct, although precluded from wrongfulness under conditions of countermeasures, may subtly chip away at the rule's legitimacy in the broad international community. A State undertaking a countermeasure, especially if successful, would seem more likely to repeat, and even adopt as a matter of policy, its willingness to breach international law norms. Similarly, once the figurative seal, so to speak, on international law breaches has been broken, officials, lawyers, and agents of domestic agencies seem far more likely to consider breach as a policy option in future international relations decisions.[107] Carrying out, or even witnessing, deliberate nonobservance of international norms, whatever the justification, likely erodes identification with those norms, deteriorating whatever compliance effect their internalization had brought about. In short, countermeasures might prompt a worrisome sort of reverse internalization of international law.

Once undertaken, reversals of internalization may also extend beyond the distinct scenarios and decision makers initially involved. Actions

---

104. *See* GEORG SCHWARZENBERGER, 2 INTERNATIONAL LAW AS APPLIED BY INTERNATIONAL COURTS AND TRIBUNALS: THE LAW OF ARMED CONFLICT 453 (1968) (observing that belligerent reprisals "reverse the operation of the chief working principle behind the laws of war from positive, to negative, reciprocity").

105. Articles of State Responsibility, *supra* note 28, art. 50 (cataloging international obligations that may not be breached as countermeasures, including the prohibition on the use of force, fundamental human rights, obligations of a humanitarian character, and peremptory norms of international law).

106. Koh, *supra* note 89, at 2649 (citing KENNETH WALTZ, MAN, THE STATE, AND WAR: A THEORETICAL ANALYSIS (1959)).

107. *See* Antonio Cassese, *The Role of Legal Advisers in Ensuring that Foreign Policy Conforms to International Legal Standards*, 14 MICH. J. INT'L L. 139, 155 (1992) (arguing that "[e]very time a State elects to ignore or reinterpret an existing international standard . . . it runs the risk of being unable to invoke the rule in the future"). Professor Cassese observes, "According to most [legal advisers], it is difficult to breach clear, fundamental, and prohibitive rules, even in extreme and unusual situations." *Id.* at 154.

originally undertaken and justified as due diligence-minded countermeasures may migrate to inapposite contexts if not carefully managed. Employed as countermeasures, otherwise unlawful conduct could become part of the international community's, the State's, the agency's, or an individual's tactical and operational playbook. Legal analyses premised on countermeasure doctrine present a danger of becoming untethered from their original conditions, and like the policies they support, may migrate to new, unintended international relations contexts. Recent experience bears out the hazard of unintended migrations of legal reasoning. Although not undertaken as countermeasures, controversial and arguably unlawful Guantanamo Bay-detention interrogation standards and their accompanying legal analyses are thought to have migrated to other theaters of U.S. government operations in which their use was unequivocally unlawful.[108]

Additionally, countermeasures may incentivize development of physical and technical means by which to breach international law. The technical and intelligence requirements for a cyber countermeasure may not in all cases involve off-the-shelf commodities. It is foreseeable that a countermeasure cyber scenario would require idiosyncratic code or supporting intelligence not ordinarily on hand. Once such means and expertise are at hand they may, as Justice Jackson observed, "lie[] about like a loaded weapon."[109] And once employed, these means are likely to become more familiar, reducing uncertainties and other prudential barriers to their use.

Of course, concerns that countermeasures may compromise respect for international law are not new or peculiar to due diligence-minded countermeasures. During the effort to produce the Articles of State Responsibility (the Articles), some States expressed concern that codification of a countermeasures regime would embolden their use with destabilizing effects.[110] Members of the International Law Commission who produced the Articles and outside commentators observed that, ironically, the Articles' approach to countermeasures might permit more aggressive forms of self-help by States.[111] Academic work has been conducted to test the institutional-internalization phenomena associated with constructivist explanations of international law compliance by States.[112] Yet the extent to which episodes

108. U.S. DEP'T OF DEF., REVIEW OF DEPARTMENT OF DEFENSE DETENTION OPERATIONS AND DETAINEE INTERROGATION TECHNIQUES, UNCLASSIFIED EXECUTIVE SUMMARY 6–7 (Mar. 7, 2005) (concluding that in early 2003, interrogation techniques intended only for use at Guantanamo Bay, Cuba, migrated to operations in Afghanistan where higher legal standards applied).

109. United States v. Korematsu, 323 U.S. 214, 246 (1944) (Jackson, J., dissenting).

110. Bederman, *supra* note 103, at 826 (citing State Responsibility, Comments and Observations Received from Governments, U.N. Doc. A/CN.4/488 (1998)).

111. *Id.* at 819.

112. *See, e.g.*, Morgan, *supra* note 93, at 81–82 (discussing a modern example of customary law internalization by a U.S. federal court).

of calculated noncompliance, such as that involved in resort to countermeasures, can upset internalization is not clear. More work is needed to understand these connections, but the logic seems initially sufficient to provoke legitimate concern.

B. Proliferation of Self-Help

In a manner illustrated by the scenario in Part IV above, recognition and refinement of a duty of cyber due diligence may result in more frequent resort to self-help. The international legal system infamously lacks dependable enforcement mechanisms.[113] While the United Nations Charter provides textual authority for robust enforcement of collective security norms, political reality has prevented even the Charter's rudimentary system of primary rules from operating as originally envisioned.[114] The Charter is silent on States' resort to self-help not involving the uses of force associated with self-defense, leaving interpretive space for capacious notions of self-help short of self-defense.[115] As a result, international law operates through a complex mixture of diplomacy, force, cooperation, compromise, adjudication, and perhaps especially, self-help.

In their current, underdeveloped state, norms for cyber due diligence present a difficult case for allegations of breach. A State that suffers harm resulting from another State's failure to actively monitor or regulate its cyber infrastructure could, at present, point to neither consistent State practice nor firm *opinio juris* to support a charge that the host State had conclusively violated international law. Similarly it is not perfectly clear, and indeed seems unlikely, that due diligence in cyberspace involves taking active measures to preempt or prevent harm to other States. In short, the law of due diligence is thinly supported and its specific operation in cyberspace is uncertain. The United States and other States have made vague indications that States owe one another a duty not to allow harm to emanate from cyber infrastructure on their territory.[116] Yet as the *Tallinn Manual 2.0* provisions

---

113. *See* MORGENTHAU, *supra* note 88, at 263–64 (asserting that a worldwide focus on national interests has stifled international peacekeeping efforts); WALTZ, *supra* note 88, at 88 (arguing that international systems are decentralized and anarchic).

114. *See, e.g.*, U.N. Charter arts. 41–43, 51 (establishing protocols for international use of force).

115. *See* U.N. Charter art. 51 (stating that nothing in the Charter "shall impair the inherent right of individual or collective self-defense" but not discussing any other form of self-help).

116. U.N. Secretary-General, *Developments in the Field of Information and Telecommunications in the Context of International Security*, at 19, U.N. Doc. A/66/152 (July 15, 2011). The U.S. submission asserts, "States are required to take all necessary measures to ensure that their territories are not used by other States or non-State actors for purposes of armed activities . . . against other States and their interests." *Id.* at 19. The United States reaffirmed its submission in 2012–13. *See* U.N. Secretary-General, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, at 2, U.N. Doc. A/68/98 (June 24, 2013) (reaffirming member States' commitment to reduce risk and enhance security).

addressed above indicate, the specifics of this duty remain unclear and elusive. Thus, at present, States should allege breaches of the duty of due diligence with respect to cyber infrastructure cautiously and should resort to countermeasures in such circumstances with even greater caution.

Refinements to and further consensus on a duty of cyber due diligence may reduce uncertainty and risk for States suffering harm. However, it is not clear that more precise or more refined norms of due diligence would produce the stability desired. In fact, it is entirely possible that refined norms of due diligence will simply result in more States being in a condition of breach. For instance, part of a refined conception of diligence might involve a duty to monitor cyber traffic for malicious content or patterns of use. There may be attractive, harm-reducing results from such a duty. But the technical feasibility of such a duty remains doubtful in the case of many States, especially developing States. In such a case, addition or refinement of a duty of monitoring might simply increase occasions of breach, increasing, in turn, occasions for resort to self-help by other States. It is easy to envision devolution into tit-for-tat exchanges of countermeasures or even reprisals. To paraphrase Geoffrey Best on the law of war during the First World War, due diligence might represent an "aid to vilification" rather than a meaningful restraint on conduct.[117]

C. Costs to Multilateral Approaches

Third, States that are better armed with legal justifications to claim and redress through self-help injuries from other States' failures of diligence in cyberspace may be reluctant to build or bolster multinational, collective solutions. It seems the more often a State resorts to countermeasures, the more likely that State will develop the capabilities and competencies required to look out for itself. A technically advanced State that aggressively tends to its interests and international law rights might be expected to develop an institutional architecture and culture to support regular resort to countermeasures. That State might be less likely to develop and resort to outside legal and technical institutions such as tribunals or arbitral mechanisms or collective technical response teams. Such a State might also be less likely to prioritize sharing threat intelligence with other States and institutions. To the extent that State achieves competitive advantage from this self-help institutional design, it might be expected to be ambivalent or even hostile to multilateral efforts to level the response playing field. If a refined duty of cyber due diligence presents greater occasions of breach and resulting countermeasures, States may be reluctant to invest the political, diplomatic, and personal capital required to develop collective response structures. Efforts to develop international approaches to cybersecurity, such

117. GEOFFREY BEST, WAR AND LAW SINCE 1945 47 (1994).

as the U.N. annual Group of Government Experts (GGE) meetings, have seen only fitful progress. Rather than close the gaps between participating States, it is foreseeable that a duty of due diligence would only highlight and exacerbate what separates the GGE from consensus and cooperation.

D. Flawed Assignment of Culpability

Finally, by evading attribution for the acts in question and focusing simply on the fact of emanation from or transit through State territory, cyber due diligence misses the mark with respect to culpability. In the scenario described above, the victim State's resort to countermeasures may interrupt the cyber harm suffered. Although perhaps effective at momentarily addressing harm, the cyber due diligence approach remains a *proxy* approach. Countermeasures grounded in due diligence breaches may achieve a general deterrent effect against other actors considering harm against that State. However, the responsible actor evades the countermeasures so long as attribution is frustrated.

The generally fungible nature of cyber infrastructure also reduces effectiveness of due-diligence-inspired countermeasures. A countermeasure undertaken to induce the cyber diligence required to halt harm may indeed inspire the target of the countermeasures to clean up its act. But it is not certain that the harm suffered by the injured State will actually cease. The malicious actor, State or non-State, may simply relocate or reroute efforts to the next nondiligent State's cyber infrastructure. This phenomena would also likely highlight the previously mentioned problem of widening the gap between States that are technologically capable and those that are not, as the more capable are less likely to be used by malicious actors, and therefore more likely to be targeted by countermeasures. Despite its difficulties, attribution, both personal and technical, remains essential to addressing malicious cyber activity. Only responses to cyber harm that accurately establish attribution present long-term, sustainable solutions.

VI. Conclusion

Turnus and Aeneas meet in the final battle of the *Aeneid*. Their colossal brawl is initially even, but Aeneas soon gains the upper hand. Disarmed and pursued by Aeneas, Turnus overestimates his remaining strength and attempts to hurl an enormous boulder at Aeneas. When the stone falls harmlessly short, Aeneas brings down the exhausted Turnus with a spear. Before Aeneas kills him, Turnus holds out his right hand and utters,

> Clearly I earned this, and I ask no quarter.
> Make the most of your good fortune here.
> . . .
> Lavinia is your bride. But go no further
> Out of hatred.[118]

A tempestuous spirit and vengeful mind, rather than King Latinus's well-meaning speech, propelled Turnus to his ill-fated combat with Aeneas. Still, rather than quell Turnus's fury, Latinus's lecture surely served to hasten rather than abate his doom.

Whether a refined duty of cyber diligence would cure or inflame the ills of cyberspace is still unclear. We are in the early days of cyber due diligence and, frankly, of the relationship between international law and cyberspace. There is some evidence of State interest in refining international law to better address the threats posed by cyberspace generally and even cyber incitements to violence particularly. In recent remarks, U.S. State Department Legal Advisor Brian Egan observed,

> [A]ll governments must work together to target online criminal activities—such as illicit money transfers, terrorist attack planning and coordination, criminal solicitation, and the provision of material support to terrorist groups. U.S. efforts to prevent the Internet from being used for terrorist purposes also focus on criminal activities that facilitate terrorism, such as financing and recruitment, not on restricting expressive content, even if that content is repugnant or inimical to our core values.[119]

The extent to which and how international law regulates cyber harm remains a pressing question. Preserving what is good about cyberspace, especially its capacity to connect far-flung people and ideas, while tempering its capacity to disrupt and harm international relations will obviously prove one of the most important challenges of the twenty-first century. Public international law offers important principles and doctrine to regulate harmful uses of cyberspace by States. However, exactly how existing international legal doctrine should be applied or adapted to operate in cyberspace is less obvious. Initially attractive solutions, such as developing a cyber duty of diligence, may contribute to short-term stability and offer attractive self-help options to States. Yet equal attention should be paid to the potentially destabilizing and long-term structural costs of such solutions.

---

118. THE AENEID, *supra* note 1, ll. 1266–76, at 402.

119. Brian J. Egan, Legal Adviser of the U.S. State Dep't, Remarks on International Law and Stability in Cyberspace at Berkeley Law School (Nov. 10, 2016) (transcript available at https://www.law.berkeley.edu/wp-content/uploads/2016/12/egan-talk-transcript-111016.pdf [https://perma.cc/B6TH-232L]).

In short, by presenting more opportunities for more States to allege more breaches of international law, due diligence potentially increases the frequency of States' resort to countermeasures and their accompanying potentially destabilizing effects. Before fully embracing a more refined notion of cyber due diligence and the consequent increased opportunities to allege breach, States are well advised to consider carefully both practical limitations of the international regime of self-help and associated costs to international stability.

* * *

Did Russian Cyber Interference in the 2016 Election Violate International Law?

Jens David Ohlin*

Introduction

Sovereignty is a funny thing. It is allegedly the foundation of the Westphalian order, but its exact contours are frustratingly indeterminate. When it was revealed that the Russian government interfered in the 2016 U.S. presidential election by, among other things, hacking into the e-mail system of the Democratic National Committee (DNC) and releasing its e-mails, international lawyers were divided over whether the cyber attack violated international law. President Obama seemingly went out of his way to describe the attack as a mere violation of "established international norms of behavior" and pointedly declined to refer to the cyber attacks as a violation of international *law*.[1]

Some international lawyers were more willing to describe the cyber attack as a violation of international law.[2] However, identifying the exact legal norm that was contravened turns out to be harder than it might otherwise appear. To the layperson, the Russian hacking constituted an impermissible (and perhaps) shocking interference in the American political process—an intervention that nonlawyers would not hesitate to label a "violation of sovereignty" as that term is used in political or diplomatic discourse.[3] The problem arises when one attempts to translate that commonsense intuition into legal discourse. At that point, the translation effort breaks down for a variety of reasons.

The genesis of the difficulty is that none of the standard rubrics for understanding illegal interventions clearly and unambiguously apply to the

---

* Associate Dean for Academic Affairs and Professor of Law, Cornell Law School.

1. Press Release, The White House, Office of the Press Secretary, Statement by the President on Actions in Response to Russian Malicious Cyber Activity and Harassment (Dec. 29, 2016), https://obamawhitehouse.archives.gov/the-press-office/2016/12/29/statement-president-actions-response-russian-malicious-cyber-activity [https://perma.cc/T6UC-6K2Z]. One reason Obama may have been unwilling to describe the attack as illegal was because the U.S. government might want the flexibility to conduct similar operations in the future, without conceding that they are illegal.

2. *See, e.g.*, Steven J. Barela, *Cross-Border Cyber Ops to Erode Legitimacy: An Act of Coercion*, JUST SECURITY (Jan. 12, 2017), https://www.justsecurity.org/36212/cross-border-cyber-ops-erode-legitimacy-act-coercion/ [https://perma.cc/UKH6-JDSQ] (arguing that Russian intervention in the 2016 presidential election was an act of coercion violating international law). It is also beyond question that the cyber attack violated various American statutes, including, possibly, 18 U.S.C. § 2701.

3. For a discussion, see Sean Watts, *International Law and Proposed U.S. Responses to the D.N.C. Hack*, JUST SECURITY (Oct. 14, 2016), https://www.justsecurity.org/33558/international-law-proposed-u-s-responses-d-n-c-hack/ [https://perma.cc/J2MM-XXMC].

facts in question. For example, the Russian interference could simply be viewed as an act of espionage, but it has long been understood (at least until recent controversies in human rights law) that spying violates domestic—but not international—law. An alternative rubric would focus on the intervention aspect of Russia's behavior. The problem here is that the standard—though by no means universally accepted—definition for what counts as an illegal intervention requires doctrinal elements such as coercion that may not be present in this case. So too with regard to the notion of an illegal "usurpation of an inherently governmental function,"[4] a legal description that is a poor fit for Russia's hacking during the 2016 election, for reasons that will be more fully articulated below.

That being said, it would be a mistake to hastily reject our commonsense intuitions about the impropriety of Russian hacking during the election. The lack of fit with the doctrinal requirements for an illegal intervention against another State's sovereignty is simply an indication that the notions of "sovereignty" and "intervention"—though mainstays of contemporary public international law doctrine—are poorly suited to analyzing the legality of the conduct in this case. A far better rubric for analyzing the behavior is the notion of self-determination, a legal concept that captures the right of a people to decide, for themselves, both their political arrangements (at a systematic level) and their future destiny (at a more granular level of policy). It is precisely this more basic right of self-determination that was violated by Russia's conduct. Unfortunately, the right of self-determination has largely lain fallow since the global process of decolonization was completed,[5] with the exception of a few cases of controversial secessions.[6] But the Russian hacking campaign is evidence that self-determination's departure from the scene in international law should be mourned and, if possible, reversed because there are situations and cases where the best legal categories for understanding the situation are not sovereignty and intervention but rather the frustratingly imprecise notion of self-determination.[7]

Accordingly, this Article proceeds in three parts. Part I will analyze the law of espionage and spying, which are widespread practices in today's

4. TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS 23 (Michael M. Schmitt & Liis Vihul eds., 2017) [hereinafter TALLINN MANUAL 2.0].

5. For a longer discussion of this phenomenon, see Jens David Ohlin, *The Right to Exist and the Right to Resist*, *in* THE THEORY OF SELF-DETERMINATION 70, 72 (Fernando R. Teson ed., 2016) (describing self-determination as "a right that is universally recognized as central and indisputable in international law, but unfortunately of very little practical significance").

6. For an example where self-determination played an important role in the legal analysis, see Reference re Secession of Quebec, [1998] 2 S.C.R. 217, 222 (Can.) (denying Quebec's claims that it had the right to secede under international law because self-determination allows secession only when "a people" is governed as part of a colonial empire; subject to alien subjugation, domination, or exploitation; or possibly when denied any meaningful exercise of self-determination).

7. *See* Edward A. Laing, *The Norm of Self-Determination, 1941-1991*, 22 CAL. W. INT'L L.J. 209, 221 (1991) (noting that the vague notion of self-determination had only been applied in colonialist contexts).

world. Though spying was once condemned as illegal under international law, that historical mistake has been rectified, and most international lawyers agree that spying violates domestic rather than international law. Part I will then query whether spying violates a human right to privacy, an argument that suggests that the Russian hacking might have violated international human rights law. Part I will conclude by outlining the obstacles to this argument.

Part II will focus on impermissible interventions against sovereignty and in particular on the requirement of coercion. The concept of coercion can be defined narrowly or broadly, with huge consequences for the outcome of the analysis in this case. Unfortunately, there is little in international law that outlines a complete theory of coercion—for that, one must look to philosophy. Finally, Part III will offer a conceptual argument that seeks to recast the sovereignty argument with a new legal architecture built from the raw materials of self-determination. The result of the argument is that the Russian cyber intervention in the 2016 election may very well have violated international law, but not for the reason that most lawyers assume. In making these arguments, the Article will make extensive reference to the *Tallinn Manual on Cyber Operations*, which offers the most up-to-date guidance on the law of cyber activities under international law.[8] Although some of the *Manual*'s statements and conclusions of law are controversial, it is nonetheless undeniable that the document is the most complete rendering of an emerging (but not universal) consensus regarding the law in this area.

One final methodological point is in order. This Article assumes that the facts currently in the public domain, and as reported by the U.S. intelligence agencies,[9] are accurate. This Article is not the right place to conduct an independent analysis of the factual underpinning of the intelligence assessment. Moreover, some facts will simply be assumed. This Article will assume that the hacking involved State action on the part of the Russian government, as opposed to private behavior. Also, this Article will assume that the attribution requirement is satisfied and that there is sufficient evidence to link the hacking with the Russian government. Moreover, in conducting the legal analysis, it is important to look at the entire event together rather than segmenting the Russian cyber interference into isolated behaviors. It is not just that the Russian government engaged in cyber intrusions against the DNC, that they disclosed e-mails to WikiLeaks, that they distributed the e-mails, that they did not engage in the same activity to the Grand Old Party, and that they deployed other cyber resources to spread fake news stories on social media. It is *all of it* taken together that paints an

8. TALLINN MANUAL 2.0, *supra* note 4, at 1.

9. *See generally* OFFICE OF DIR. OF NAT'L INTELLIGENCE, ASSESSING RUSSIAN ACTIVITIES AND INTENTIONS IN RECENT US ELECTIONS (Jan. 6, 2017) [hereinafter ASSESSING RUSSIAN ACTIVITIES].

entire picture of cyber interference in the 2016 election. It is this total picture that will be evaluated in this Article.

I. Spying, Surveillance & Privacy

One obvious way of analyzing the Russian intervention is to focus exclusively on the illicit and unauthorized access to specific computer networks and specific e-mail accounts—access that sounds like spying under a layperson's definition of spying. However, while spying is clearly a violation of U.S. law, it is a separate question whether it is a violation of international law, which has a more limited scope.

A. Spying Under International Humanitarian Law

In 1942, the U.S. Supreme Court upheld the conviction at a military commission of Nazi operatives who landed on the east coast of the United States with orders to proceed covertly across the homeland to sabotage key civilian and military installations.[10] In its decision, the Supreme Court noted,

> The spy who secretly and without uniform passes the military lines of a belligerent in time of war, seeking to gather military information and communicate it to the enemy, or an enemy combatant who without uniform comes secretly through the lines for the purpose of waging war by destruction of life or property, are familiar examples of belligerents who are generally deemed not to be entitled to the status of prisoners of war, but to be offenders against the law of war subject to trial and punishment by military tribunals.[11]

With this phrase, the Supreme Court seemed to convey that spies were subject to the jurisdiction of military commissions because spying violates the international law of war.

Over time, most international lawyers have come to view the *Quirin* holding as resting on a mistaken assumption, insofar as it relies on the notion that spying represents a violation of the international law of war. Richard Baxter, in his famous article on spies, saboteurs, and guerillas, spoke for a scholarly consensus when he concluded that the *Quirin* Court had suffered from a basic but understandable confusion: the difference between a violation of international law and a violation of domestic law that is unprivileged under international law.[12] Spying falls into the latter category, not the former.[13]

---

10. *Ex parte* Quirin, 317 U.S. 1, 21–23, 48 (1942).

11. *Id.* at 31.

12. RICHARD BAXTER, *So-Called 'Unprivileged Belligerency': Spies, Guerrillas, and Saboteurs*, *in* HUMANIZING THE LAWS OF WAR: SELECTED WRITINGS OF RICHARD BAXTER 37, 44 (Detlev F. Vagts et al. eds., 2013).

13. This issue is also raised by the appellate litigation in *Al Bahlul*, which concerns the applicability of the conspiracy charge before military commissions. *See* United States v. Al Bahlul, 820 F. Supp. 2d 1141, 1167, 1183 (U.S.C.M.C.R. 2011), *vacated*, No. 11-1324, 2013 WL 297726 (D.C. Cir. Jan. 25, 2013), *aff'd in part, vacated in part*, 767 F.3d 1 (D.C. Cir. 2014), *vacated in part*,

B. Privacy Under Human Rights Law

The established view that spying is not a violation of international law has recently come under attack from human rights lawyers who note that the right to privacy is protected by international and European human rights law. For example, Article 17 of the ICCPR states that "[n]o one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation."[14] According to this provision, it would seem as if Russia's cyber intrusion violated the human rights of the owners of the various e-mail accounts, including John Podesta and several DNC officials. Indeed, the reference in Article 17 to "correspondence" would seem to be especially relevant to this case.

International lawyers studying intelligence surveillance were late to recognize the significance of Article 17 and similar provisions in other human rights instruments protecting the right to privacy. However, with the revelation of global surveillance efforts by the National Security Agency and similar agencies in other countries—some of which were disclosed by Edward Snowden—human rights activists have harnessed international human rights law as a potential rubric with which to resist mass-surveillance efforts.[15] If these provisions apply, they may suggest that the legal status of spying may have changed since the time of *Quirin*. Despite the fact that spying is a widespread or even universal tool of statecraft, the adoption of the ICCPR and ECHR may have outlawed the practice.

However, there are several obstacles to this "spying as a violation of the right to privacy" argument. First, human rights provisions were originally conceptualized as constraints against a government's conduct towards its own citizens.[16] So, for example, Article 17 would constrain and prohibit Russian attempts to spy on its own citizens, or U.S. attempts to spy on Americans—at least if they are arbitrary or unlawful (lawful or nonarbitrary spying, i.e., authorized by domestic statute, would not necessarily be covered

---

792 F.3d 1 (D.C. Cir. 2015), *vacated en banc*, 840 F.3d 757 (D.C. Cir. 2016). At issue is how to read the *Quirin* precedent, given the Court's confusion between international offenses and domestic offenses that are unprivileged. One way of reading *Quirin* is that the Court upheld jurisdiction of military commissions for domestic offenses (because spying is a domestic offense). Another way of reading the case is that the Court upheld jurisdiction of military commissions for international offenses only, because the Court was laboring under the mistaken view that spying was a direct violation of international law.

14. International Covenant on Civil and Political Rights art. 17, Dec. 19, 1966, S. EXEC. DOC. E (1978), 999 U.N.T.S. 171 [hereinafter ICCPR].

15. The *Tallinn Manual* recognizes that human rights law may be a constraint on cyber-related activities. *See* TALLINN MANUAL 2.0, *supra* note 4, at 316. However, its statements relate mostly to surveillance *within* the territorial State, rather than extraterritorial surveillance. *See id.*

16. LOUIS HENKIN, THE AGE OF RIGHTS 37 (1990) ("Acting with other States (the State as legislator), each State agrees to recognize and give legal status in the international system to 'human rights' as claims that every individual has—or should have—upon his or her own society.").

by the provision). In the 2016 election, the spying by Russia targeted American citizens, and it is unclear whether the Article 17 right to privacy was meant to cover such transnational conduct.

The second problem is that foreign spying is so widespread that customary international law arguably does not prohibit it. There are two responses to this objection. The first is that a customary international law analysis should not displace a treaty-based analysis. So whether spying violates customary international law does not answer whether spying violates a particular treaty provision. This is a common problem with international law discourse—the tendency to evaluate all conduct under the rubric of customary international law, even if a treaty covers the conduct. Often, these invocations of customary international law are purportedly justified by claims that customary international law runs parallel to the treaty provisions. But even if that were the case, the conduct only needs to be illegal according to one source of international law.

The other response is an appeal to "the subsequent practice of the parties"—a doctrine that encourages reference to the practice of States as a means of treaty interpretation.[17] Under this methodology, the fact that States all engage in spying—and rarely criticize it as illegal—could be relevant for an interpretation of Article 17 and other treaty provisions. Unfortunately, this methodology is vastly overused in contemporary legal discourse; it is objectionable because it threatens to transform treaty interpretation into a kind of ersatz customary international law analysis (based on State practice). State practice is important but only when the norm flows from custom; when a norm flows from treaty law, State practice ought to fade in relevance. Indeed, even under the interpretive doctrine of the "subsequent practice of the parties," the method should only be used when it is clear that the parties are acting pursuant to the treaty—in all other cases the practice of the parties is not a relevant method for analyzing an ambiguous treaty provision.[18] This methodology seems especially ill-suited to analyzing human rights treaties, which demonstrate a unique structure that is not at all analogous to the typical bilateral arrangement. Human rights treaties are multilateral conventions that have *individuals* as their primary beneficiaries. The fact that most nations ignore their obligations under particular human rights provisions ought not to be an argument that the conduct therefore does not violate a human rights

17. Luigi Crema, *Subsequent Agreements and Subsequent Practice Within and Outside the Vienna Convention*, *in* TREATIES AND SUBSEQUENT PRACTICE 13, 14–18 (Georg Nolte ed., 2013) (discussing the origins and interpretive frameworks of "the subsequent practice of the parties").

18. *See* Georg Nolte (Special Rapporteur), Int'l L. Comm'n, Second Report on Subsequent Agreements and Subsequent Practice in Relation to the Interpretation of Treaties, ¶¶ 4–11, U.N. Doc. A/CN.4/671 (Mar. 26, 2014) (defining "in the application" and "regarding the interpretation" of the treaty).

obligation.[19] That conclusion would turn human rights treaties on their head by whitewashing widespread noncompliance and transforming it into compliance by redefining the relevant norm.[20]

At the end of the day, treaty interpretation is different from customary international law, and ought to be. Although State practice can be relevant for treaty interpretation under the rubric of subsequent practice of the parties, there are substantial constraints on the application of this methodology.[21] Moreover, it is not at all clear that the subsequent practice of States ought to be relevant in the context of human rights treaties, where the ultimate beneficiary of the relevant provision are individuals per se, whose subsequent practice would be largely ignored under a putative rule that allows a subsequent practice of widespread noncompliance to effectively gut the core of important human rights provisions codified in binding human rights instruments.

C. Extraterritorial Obligations Under Human Rights Law

The bigger problem with concluding that Russian spying during the 2016 election violated the ICCPR is the question of the treaty's extraterritorial scope. The ICCPR requires:

> Each State Party to the present Covenant undertakes to respect and to ensure to all individuals within its territory and subject to its jurisdiction the rights recognized in the present Covenant, without distinction of any kind, such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status.[22]

The question is the proper scope of the qualification "to all individuals within its territory and subject to its jurisdiction."[23] One interpretation is that this qualification applies to both the obligation to respect and the obligation to ensure. This suggests that the treaty has little or no extraterritorial scope.

---

19. For a similar argument, see Sean D. Murphy, *The Relevance of Subsequent Agreement and Subsequent Practice for the Interpretation of Treaties*, *in* TREATIES AND SUBSEQUENT PRACTICE 82, 91 (Georg Nolte ed., 2013) (suggesting that human rights tribunals may shy away from the subsequent practice methodology because it would diminish rather than enhance human rights norms).

20. An overreliance on practice also has the opposite problem as well. If States are engaging in a particular practice, it does not automatically mean that the practice demonstrates that they are required to engage in the activity. *See, e.g.*, Certain Expenses of the United Nations, Advisory Opinion, 1962 I.C.J. Rep. 197, 201–02 (July 20) (separate opinion of Fitzmaurice, J.) (arguing that voluntary State expenditures do not imply an obligation for such spending).

21. For example, Nolte argues that "[t]he examples from the case law and State practice substantiate the need to identify and interpret carefully subsequent agreements and subsequent practice, in particular to ask whether the parties, by an agreement or a practice, assume a position regarding the interpretation of a treaty, or whether they are motivated by other considerations." Nolte, *supra* note 18, at 11.

22. ICCPR, *supra* note 14, art. 2.

23. *Id.*

In other words, Russia has an obligation to respect and ensure the right to privacy of individuals within its territory, which would exclude DNC officials living in the United States.

Some human rights scholars have recently suggested that this narrow reading of Article 2 is far too restrictive. They suggest that the phrase "to all individuals within its territory and subject to its jurisdiction" applies only to the obligation to ensure, and that by contrast, the obligation "to respect" is territorially unbounded and applies across the globe.[24] If this view is correct, then Russia has an obligation to respect the privacy of all individuals around the world (and then has the further obligation to "ensure" this right to those living in Russia). But the more basic obligation applies universally. If this is true, the hacking violated the ICCPR.

The problem with the U.S. asserting this reading of the ICCPR is that the U.S. insists that the ICCPR does not have this broad extraterritorial scope. This legal question was the subject of intense interdepartmental dispute toward the end of the Obama Administration. The longstanding view of the U.S. government has been that most provisions of the ICCPR do not apply extraterritorially.[25] In 2010, State Department Legal Advisor Harold Koh authored a memorandum that argued that this established view was wrong and that the legal argument in favor of extraterritoriality ought to be given greater credence.[26] Ultimately, though, after pushback from other executive agencies, the Administration did not adopt the Koh memorandum as official U.S. legal policy. If Koh is right, though, this would provide one avenue through which to view the Russian interference as unlawful, i.e., a violation of international human rights law. However, it is not an argument that the U.S. will adopt anytime soon—at least not until it changes its position on the extraterritorial scope of human rights obligations.

---

24. *See* MARKO MILANOVIC, EXTRATERRITORIAL APPLICATION OF HUMAN RIGHTS TREATIES: LAW, PRINCIPLES, AND POLICY 18 (2011) (describing the difference between two types of State obligations, the negative obligation to "respect" and the positive obligation to "ensure" human rights).

25. *See* U.N. Human Rights Comm'n, 53d Sess., 1405th mtg. ¶ 20, U.N. Doc. CCPR/C/SR 1405 (Apr. 24, 1995) (State Department Legal Advisor Conrad Harper stating, "The Covenant was not regarded as having extraterritorial application [by the U.S. government]. In general, where the scope of application of a treaty was not specified, it was presumed to apply only within a party's territory"); *see also* U.N. Human Rights Comm'n, Consideration of Reports Submitted by States Parties Under Article 40 of the Covenant, ¶ 469, U.N. Doc. CCPR/C/USA/3 (Nov. 28, 2005) ("The United States continues to consider that its view is correct that the obligations it has assumed under the Covenant do not have extraterritorial reach.").

26. U.S. Dep't of State, Office of the Legal Adviser, Memorandum Opinion on the Geographic Scope of the International Covenant on Civil and Political Rights, at 4 (Oct. 19, 2010) ("[T]he Covenant *does* impose certain obligations on a State Party's extraterritorial conduct under certain circumstances.").

II. Violations of *Domaine Réservé*

The more likely and potentially fruitful rubric for analyzing the Russian cyber interference with the 2016 election is the concept of sovereignty. Under bread-and-butter principles of public international law, States are prohibited from interfering with another State's sovereignty. These actions can be understood as either an "interference" against another State's sovereignty or as an illegal "usurpation" of a State's inherently governmental power.[27] Either way, both avenues flow from the basic building blocks of sovereignty. As this Part demonstrates, however, the technical requirements for an illegal intervention might not apply to the Russian intervention, depending on how one understands the concept of coercion.

A. The Concept of Domaine Réservé

When speaking about the general prohibition against interfering with another State's sovereignty, public international lawyers often refer to a State's *domaine réservé*, its exclusive power to regulate its internal affairs without outside interference.[28] Indeed, the notion of *domaine réservé* would seem to be constitutive of the descriptive and normative uses of the phrase "sovereignty," in the sense that being a sovereign State naturally entails the power to act as the sovereign.[29] This is the enduring notion of sovereign prerogative.

Unfortunately, despite the patina of precision in its French rendering, the concept has little internally generated content. It has to be spelled out with reference to theories and concepts that are external to the notion of

---

27. *See* TALLINN MANUAL 2.0, *supra* note 4, at 20. The *Tallinn Manual* explains that sovereignty can be violated by an intervention against or usurpation of a State's essential functions:

> The second basis upon which the Experts determined a violation of sovereignty occurs is when one State's cyber operation interferes with or usurps the inherently governmental functions of another State. This is because the target State enjoys the exclusive right to perform them, or to decide upon their performance. It matters not whether physical damage, injury, or loss of functionality has resulted or whether the operation qualifies in accordance with the various differing positions outlined above for operations that do not result in a loss of functionality.

Id. at 21–22 (footnote omitted).

28. Galina G. Shinkaretskaya, *Content and Limits of 'Domaine Réservé', in* INTERNATIONAL LAW AND MUNICIPAL LAW: PROCEEDINGS OF THE GERMAN–SOVIET COLLOQUY ON INTERNATIONAL LAW AT THE INSTITUT FÜR INTERNATIONALES RECHT AN DER UNIVERSITÄT KIEL, 4 TO 8 MAY 1987, 123, at 123–24 (Grigory I. Tunkin & Rüdiger Wolfrum eds., 1988); *see also* TALLINN MANUAL 2.0, *supra* note 4, at 15, 314–17 (discussing the relationship between sovereignty and *domaine réservé*).

29. *See* Shinkaretskaya, *supra* note 28, at 124–25 (discussing the U.N. Declaration of Principles and limits of domestic sovereignty); *see also* G.A. Res. 2625 (XXV), annex, Declaration on Principles of International Law Concerning Friendly Relations and Co-Operation Among States in Accordance with the Charter of the United Nations, pmbl. (Oct. 24, 1970) (detailing principles of noninterference in the affairs of other States but noting that States have the duty to refrain from forcible actions that deprive peoples of their rights to self-determination, freedom, and independence).

sovereignty. The notion of sovereign prerogative has limits, and almost every international lawyer would agree with this. The question is where to locate the limit—which domains or activities should be off-limits because they fall within a State's *domaine réservé* and which domains are subject to foreign action.

The *Tallinn Manual* argues that an intervention against a State's choice of political structure would count as an infringement against its *domaine réservé*, but only in the case where the intervention is accompanied by some degree of coercion. So, for example, the drafters of the *Tallinn Manual* do not view the spreading of propaganda as, by itself, indicative of an illegal intervention against another State's *domaine réservé*.[30] In prior international conflicts, the United States and other countries have dropped leaflets on the territory of another State in order to convince a foreign population to pressure its leaders into a course of action.[31] The Voice of America broadcasts across the globe in order to provide information to foreign audiences. The government of South Korea places loudspeakers near the border with North Korea in order to disseminate news and information that might not otherwise reach its epistemically isolated population.[32] No one denies that Putin would have been permitted to speak publicly on Russia Today, the decidedly pro-Putin State television network, and declare his support for Trump and urge all Americans to vote for him. This right to engage in the political process is hardly a violation of America's *domaine réservé*.

B. The Requirement of Coercion

In order to find that there was an impermissible intervention, the *Tallinn Manual* points to the requirement of coercion, a doctrinal element that flows from the *Nicaragua* judgment.[33] In order to count as illegal intervention, the

---

30. TALLINN MANUAL 2.0, *supra* note 4, at 26.

> [T]he International Group of Experts agreed that [propaganda] transmission into other States is generally not a violation of sovereignty. However, the transmission of propaganda, depending on its nature, might violate other rules of international law. For instance, propaganda designed to incite civil unrest in another State would likely violate the prohibition of intervention (Rule 66). Similarly, propaganda by a vessel in transit through the territorial sea renders the passage noninnocent (Rule 48).

Id.

31. *See* BARAK KUSHNER, THE THOUGHT WAR: JAPANESE IMPERIAL PROPAGANDA 151 (2006) (detailing the leafletting campaign undertaken by the United States in the Pacific Theater of World War II); HISTORICAL DICTIONARY OF AMERICAN PROPAGANDA 160 (2004) (summarizing various propaganda efforts used by countries during World War II); THE U.S. AIR SERVICE IN WORLD WAR I, VOLUME IV: POSTWAR REVIEW 221 (1979) (noting leafletting efforts of the American Air Service during World War I).

32. Julian Ryall & Colin Freeman, *South Korea Uses Loudspeakers to Blast North Korea with 'Popaganda'*, TELEGRAPH (Jan. 8, 2016), http://www.telegraph.co.uk/news/worldnews/asia/northkorea/12088568/north-south-korea-pop-music-loudspeakers.html [https://perma.cc/2YW7-JGP3].

33. TALLINN MANUAL 2.0, *supra* note 4, at 315 n.768; Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. Rep. 14, ¶ 205 (June 27)

structure of the interaction must have the following form: engage in this action; otherwise you will suffer a particular consequence. Then, the State complies with the coercive demand because it finds the promised consequence to be intolerable to live with.

A key element here is the assumption that the threatened consequence constitutes an *illegal* or *wrongful* action. Although never stated explicitly, this assumption is arguably implicit in the *Nicaragua* judgment, in part because the court concluded that actions of the United States constituted an illegal use of force under international law. In contrast, if the threatened consequence is an action that the threatening State clearly has the authority under international law to engage in, then the action is merely an example of bald strategic behavior, not coercion per se. So, for example, in the *Nicaragua* case, the International Court of Justice concluded that the mining of the harbor waters (and support for the Contras) constituted illegal intervention because the United States did not have the right to mine the harbor and the action constituted a use of force in violation of the U.N. Charter and customary law.[34] If, on the other hand, a State mounts a naval blockade in a situation when the blockade is permissible under international law, it cannot count as an example of coercion just because the target of the blockade views the situation as intolerable and therefore capitulates. The same thing might be said of a sanctions regime where the underlying sanctions are consistent with international law. So the key to an impermissible act of coercion is that it forces the target State to act by virtue of its desire to avoid the consequences that flow from a threatening State's illegal or impermissible action.[35]

However, it is not obviously the case that the *Nicaragua* paradigm for coercion is the correct interpretation. Although there is not much law on this question in the burgeoning field of the international law of cyber operations, the issue has been raised and analyzed in numerous other fields, including domestic law and philosophy. For example, in the philosophical literature on coercion, most scholars writing in this area have assumed that what makes coercion wrongful is that the coercer threatens an outcome that makes the target worse off.[36] Some scholars argue that even conditional offers—which might make the target better off—can be coercive because they may

("Intervention is wrongful when it uses methods of coercion . . . . The element of coercion . . . defines, and indeed forms the very essence of, prohibited intervention . . . .").

34. Nicar. v. U.S., 1986 I.C.J. at 128, ¶¶ 251–52.

35. It is unclear whether a causal requirement must be satisfied. *See* TALLINN MANUAL 2.0, *supra* note 4, at 320 (noting its experts were "divided").

36. *See, e.g.*, Robert Nozick, *Coercion, in* PHILOSOPHY, SCIENCE, AND METHOD 440, 447 (Sidney Morgenbesser et al. eds., 1969) (arguing that a threat makes the consequences of a person's actions "worse than they would have been in the normal and expected course of events").

constitute an offer so good that it cannot be refused.[37] The difference between a conditional threat and a conditional offer is a nonarbitrary baseline against which we can label something as a benefit or a burden. Some scholars believe that the baseline is the "normal or natural or expected course of events,"[38] while others insist that establishing a coherent baseline will inevitably be arbitrary, and therefore that offers can be coercive.[39] Under either understanding, there is no requirement that the conditional threat or offer involve an otherwise illegal action. One prominent exception is Mitchell Berman, who concludes that wrongful coercion involves threats to engage in otherwise impermissible actions.[40] Berman's argument is that coercion is wrongful because it involves threatening to do an action which itself is impermissible; the impermissibility of the threat flows from the impermissibility of the completed action, even if it is never required (because the threat is successful).

In domestic law, coercion does not always require the threatening of a consequence that constitutes an illegal or impermissible act, i.e., something that the threatening agent is not permitted to do. Consider the U.S. Supreme Court's review of Medicaid expansion in *NFIB v. Sebelius*.[41] In *Sebelius*, the question facing the Court was whether Congress had engaged in impermissible coercion by attaching a condition to the funds that the federal government provides to States for their Medicaid programs.[42] The condition required the States to expand their Medicaid programs or risk losing federal funding for Medicaid entirely (not just for the expansion).[43] The Supreme Court had already determined, back in *South Dakota v. Dole*, that Congress could use its spending power to induce compliance by sovereign States.[44] In that case, Congress had tied federal funding for highways to the drinking age, so that States were required to raise their drinking age to twenty-one or risk losing five percent of the funding that they received from the federal

37. *See, e.g.*, Virginia Held, *Coercion and Coercive Offers*, *in* COERCION: NOMOS XIV 49, 54 (J. Roland Pennock & John W. Chapman eds., 1972) (discussing whether offers can be coercive).

38. *See, e.g.*, Nozick, *supra* note 36, at 447; *see also Coercion*, *in* STANFORD ENCYCLOPEDIA OF PHILOSOPHY (2011), https://plato.standford.edu/entris/coercion/ [https://perma.cc/KUB6-H83N].

39. *See, e.g.*, Held, *supra* note 37, at 56–57 (explaining the difficulty in defining coercion in a way that excludes the possibility of coercive offers); David Zimmerman, *Coercive Wage Offers*, 10 PHIL. & PUB. AFF. 121, 131 (1981) (proposing a framework to accommodate coercive offers without recourse to a moral baseline).

40. *See* Mitchell Berman, *The Normative Functions of Coercion Claims*, 8 LEGAL THEORY 45, 55 (2002) (defining a coercive act as an act that "involves a threat, conditioned upon specified action or inaction by a recipient of the proposal, to do what it would be impermissible . . . for the threatener to do"); Mitchell Berman, *Coercion Without Baselines: Unconstitutional Conditions in Three Dimensions*, 90 GEO. L.J. 1, 15 (2001) (basing the coerciveness of a conditional proposal on whether "it would be wrong to carry out the act threatened").

41. Nat'l Fed'n of Indep. Bus. v. Sebelius, 132 S. Ct. 2566 (2012).

42. *Id.* at 2577.

43. *Id.* at 2572.

44. South Dakota v. Dole, 483 U.S. 203, 210–11 (1987).

government for highway projects.[45] The Court ruled that these funding conditions were not unconstitutionally coercive, but did concede that prior "decisions have recognized that in some circumstances the financial inducement offered by Congress might be so coercive as to pass the point at which 'pressure turns into compulsion.'"[46] So although the funding scheme in *Dole* was constitutional, the Court reiterated its holding that the withdrawal of financial benefits could rise to the level of coercion.

In *Sebelius*, the Court declared that it had finally found a case where pressure had turned into compulsion, even though Congress was simply threatening to take away a benefit that it was under no obligation to provide in the first instance. Writing for the majority, Chief Justice Roberts declared that "[i]n this case, the financial 'inducement' Congress has chosen is much more than 'relatively mild encouragement'—it is a gun to the head."[47] But what was the gun to the head? It was simply a threat to remove all Medicaid funding to a State—something that the Constitution does not require the federal government to do in the first place. So how can it be coercive to remove something that you are not required to do in the first place?

Justice Roberts answered that, in contrast to the modest amount of highway funds that were at issue in *Dole*, the *Sebelius* funding scheme made up as much as ten percent of the State's entire budget, a consequence that constituted an "economic dragooning that leaves the States with no real option but to acquiesce in the Medicaid expansion."[48] The States, having grown accustomed (addicted?) to the higher amount of federal aid, would not be able to survive once it was withdrawn—at least not without substantial bureaucratic and financial chaos. So the majority apparently viewed the total amount as the crucial factor, not the question of whether the threatened consequence was illegal or not. At least in this limited circumstance, a court viewed coercion as applying to a case where the negative consequence was not otherwise illegal or impermissible. In essence, an offer that is too good to refuse may constitute coercion because it seems impossible for the recipient to forego the benefits in question.[49]

Applying this insight to the case of Russian cyber interference, one might argue that coercion does not necessarily require a threat to commit an

45. *Id.* at 211.

46. *Id.* (quoting Steward Machine Co. v. Davis, 301 U.S. 548, 590 (1937)).

47. *Sebelius*, 132 S. Ct. at 2604.

48. *Id.* at 2604–05.

49. The philosopher Robert Nozick argues that coercion involves the substitution of the agent's motives and intentions for the motives and intentions of the coercer. ROBERT NOZICK, PHILOSOPHICAL EXPLANATIONS 48 (1981). This insight provides an opening for explaining how the withholding of a benefit could rise to the level of coercion. In that situation, the action produced by the withholding of the benefit might stand in a closer relationship to the coercer's motives and intentions than to the target's motives and intentions. This is certainly the case with regard to the coercive Medicaid expansion, which stood in a closer relationship to Congress's intention than it did to the States' intentions.

unlawful act, in the sense in which *Nicaragua* implies or Berman argues. The *sine qua non* of coercion is that the threat compelled the State to act in a way that it otherwise would not act,[50] not that the threatened consequence was illegal.[51] If the Russian hacking constituted "threatening conduct," the lack of a threatened consequence that is independently illegal should not be taken as a fatal defect to the argument.

Even so, there are substantial impediments to concluding that the Russian hacking in the 2016 election constituted illegal coercion—impediments that raise a series of broader questions about the entire episode. A legal finding of coercion would depend on identifying some individual or group as the target of the coercion. Was it the American voters? Were they coerced into voting for Trump and not for Clinton? If so, what were the threatened consequences? One might argue that the Russian intervention came with an implied threat to withhold benefits if Hillary Clinton were elected and that Russia would act in a more cooperative manner towards the United States if Trump were elected, perhaps in exchange for reciprocal considerations from a new Trump Administration. Or perhaps one might argue that the hacking came with the threat of future illegal behavior on the part of the Russian government: either more instances of hacking, or more daringly, increased military aggression in places like Crimea or eastern Ukraine. Or, one might assume that the object of the coercion was actually Hillary Clinton. In that regard, perhaps the point was that Clinton was implicitly informed that she should adopt a more conciliatory attitude toward Russia (and drop any attempts to pursue regime change in Russia or oust Putin), and that if she did not comply, the hacking of DNC e-mails would be the threatened consequence.[52] However, it is unclear if this threat or offer was made, either explicitly or implicitly. Furthermore, it is also unclear whether one should equate the American electorate with the "State" itself.

Certainly, the question of whether there was coercion in this case should be determined holistically based on the facts surrounding the intervention,

---

50. *See* TALLINN MANUAL 2.0, *supra* note 4, at 319 ("The key is that the coercive act must have the potential for compelling the target State to engage in an action that it would otherwise not take (or refrain from taking an action that it would otherwise take).").

51. This would imply that a retorsion is inherently coercive; it is not clear whether international lawyers would be comfortable with that conclusion.

52. It is certainly the case that coercion need not be direct and may come in an indirect form:

> Coercion sufficient to support a finding of unlawful intervention may take either a direct or indirect form. In its findings of fact, the International Court of Justice in the *Nicaragua* judgment determined that the United States had supplied assistance to rebels, including "training, arming, equipping . . . [rebel] military and paramilitary actions in and against Nicaragua." The court held that the principle of non-intervention "forbids all States or groups of States to intervene directly or indirectly in internal or external affairs of other States."

TALLINN MANUAL 2.0, *supra* note 4, at 319–20.

rather than hewing formalistically to abstract requirements.[53] Other scholars have concluded that the Russian hacking included some coercive element, implicitly rejecting the requirement of an impermissible consequence.[54] One possibility for defining coercion is simply the scale and effect of the overall intervention,[55] which in this case was quite substantial. This is perhaps the most important lesson of the *Sebelius* reasoning, where the Court looked to the totality of the circumstances before deciding whether the actions in the case were fundamentally coercive. However, there must be a line between being coercive and being corrosive to the proper functioning of a democracy. While the Russian hacking was certainly corrosive, it is genuinely unclear whether it should count as coercive.[56]

C. *Illegal Usurpation of a Government Function*

The other possibility is that the Russian cyber hacking was illegal, not because it constituted a coercive intervention but rather an illegal "[u]surpation of an inherently governmental function,"[57] which does not require the element of coercion. The question is what was the inherently governmental function in this case.

Undeniably, the holding of a federal election is an inherently governmental function in a liberal democracy. So, in theory, the *disruption* of an election should count as the usurpation of an inherently governmental

---

53. *See id.* at 319 ("A few Experts, however, argued that it is impossible to prejudge whether an act constitutes intervention without knowing its specific context and consequences. For them, the context and consequences of a particular act that would not normally qualify as coercive could raise it to that level.").

54. For example, Steven Barela has concluded that,

> coercion can be understood as more than simply forcing an electoral outcome. The significance and expanse, both in scale and reach, of the interests targeted are relevant. Whether the Russian meddling was meant to achieve a particular result in the election (wishing to aid one candidate over another), there were also more important—even if less tangible—matters at stake.

Barela, *supra* note 2.

55. *See* Myres S. McDougal & Florentino P. Feliciano, *International Coercion and World Public Order: The General Principles of the Law of War*, 67 YALE L.J. 771, 782 (1958) (suggesting that coercion is defined by three dimensions of consequentiality, including "the importance and number of values affected, the extent to which such values are affected and the number of participants whose values are so affected"); Sean Watts, *Low-Intensity Cyber Operations and the Principle of Non-Intervention*, *in* CYBERWAR: LAW AND ETHICS FOR VIRTUAL CONFLICT 249, 257 (Jens David Ohlin et al. eds., 2015) ("[McDougal's] and Feliciano's dimensions of coercion might consider the nature of State interests affected by a cyber operation, the scale of effects the operation produces in the target State, and the reach in terms of number of actors involuntarily affected by the cyber operation."); Barela, *supra* note 2 (concluding that the McDougal and Feliciano formulation lends support to the conclusion that the Russian hacking violated international law).

56. *See also* William Banks, *State Responsibility and Attribution of Cyber Intrusions After* Tallinn 2.0, 95 TEXAS L. REV. 1487, 1501 (2017) (concluding that according "to the traditional measures, there was no coercion and no unlawful intervention" but also conceding that "because [S]tate practice and resulting customary international law is based on examples from kinetic conflicts . . . [w]e should temper our confidence in this coercion analysis").

57. *See* TALLINN MANUAL 2.0, *supra* note 4, at 24.

function. Indeed, the drafters of the *Tallinn Manual* listed a number of governmental functions, including "changing or deleting data such that it interferes with the delivery of social services, the conduct of elections, the collection of taxes, the effective conduct of diplomacy, and the performance of key national defence activities."[58] In the 2016 election, however, the Russian government allegedly *released* private information to the public, rather than "changing or deleting" it.[59] Moreover, the *Tallinn Manual* does not further define what constitutes the "conduct of elections."

Everyone agrees that had the Russian government tampered with the ballot boxes, or with electronic voting, this would count as a violation of international law, because the *counting of votes* during an election is a paradigmatically "governmental function," which in that case would be "usurped" by Russia.[60] Votes should be tabulated, counted, and reported by the government officials administering the election, and any interference with *that* process sounds like a usurpation of an inherently governmental function. At this moment in time, however, there is no publicly available evidence that the Russian cyber interference included tampering with the vote-tabulation process.[61] The interference included disclosure of private information and possibly distribution of fake news stories, falling under the umbrella of propaganda and violations of the right to privacy.[62] We are left then with an overall impression of illegal conduct, but without a clear and unambiguous doctrinal route towards that conclusion.

III. A Violation of Self-Determination

Having failed to identify an unambiguous argument that the Russian cyber interference satisfied the doctrinal requirements for an illegal intervention under international law, this section will look at the situation with reference to political terminology, in order to identify a better legal framework for analysis.[63] In political terms, the Russian hacking interfered with a key element of sovereignty, insofar as sovereignty is understood as a

58. *Id.* at 22.

59. ASSESSING RUSSIAN ACTIVITIES, *supra* note 9, at 2–3.

60. *See, e.g.*, Brian J. Egan, Legal Adviser, U.S. Dep't of State, Remarks at Berkeley Law School on International Law and Stability in Cyberspace (Nov. 10, 2016), https://www.law.berkeley.edu/wp-content/uploads/2016/12/egan-talk-transcript-111016.pdf [https://perma.cc/B6TH-232L] ("[A] cyber operation by a State that interferes with another country's ability to hold an election or that manipulates another country's election results would be a clear violation of the rule of non-intervention.").

61. ASSESSING RUSSIAN ACTIVITIES, *supra* note 9, at 3 (concluding that although Russian hackers accessed computer systems of State and local electoral boards, these systems were "not involved in vote tallying").

62. *Id.* at 4 (describing quasigovernmental trolls as "contribut[ing] to the influence campaign").

63. I am indebted to Philip Bobbitt for discussing this point with me.

relational concept that connects the government with the will of the people.[64] The whole point of democratic governance is that the government should represent the will of the people, and this relationship might be called the "sovereign will." If this is what is meant by sovereignty, then clearly the Russian hacking constituted an interference and *distortion* of the sovereign will, because the goal of the hacking was to help elect a candidate who was sympathetic to the interests of the Russian government, rather than elect a candidate who represented the hopes and desires of the American people.

This generates a translation problem. The notion of sovereign will described above does not accord with the concept of sovereignty as public international lawyers usually use the term. Of course, the word sovereignty is notoriously slippery and vague and often generates more heat than light.[65] But generally speaking, when a public international lawyer speaks of sovereignty, they mean the right of a State to control its territory, regulate its subjects, and be free from external military aggression, as well as lesser forms of impermissible interventions and interference.[66] Indeed, this is the notion of sovereignty that guided our legal analysis in Parts I and II of this Article. However, we were proceeding under the assumption that the legal notion of sovereignty—and its companion notion of unlawful interventions against sovereignty—was the proper legal framework for understanding an event that politicians and even political theorists would have analyzed with the language (their language) of sovereignty. But this assumption may be false. The best legal analogue for the political concept of sovereignty may not be the legal concept of sovereignty after all.

The reason for the translation problem is that the legal notion of sovereignty is centered around the State, while the political notion of sovereignty is not so carefully circumscribed, and often relates to the *people* whose sovereign will is represented by the government and even perhaps protected by the constitutional order.[67] To the extent that something untoward happened during the 2016 election, the relevant victim here was not the American State but rather the American *people*, whose expression of political will was interfered with. But once one shifts from discussing the State to the people, the legal language of sovereignty becomes singularly

64. For example, Rousseau would have referred to this as the "general will." *See* JEAN-JACQUES ROUSSEAU, THE SOCIAL CONTRACT AND DISCOURSES 22 (G.D.H. Cole ed. & trans., J.M. Dent & Sons 1913) (1761).

65. *See, e.g.*, Louis Henkin, *That "S" Word: Sovereignty, and Globalization, and Human Rights, Et Cetera*, 68 FORDHAM L. REV. 1, 1 (1999) (noting the misuse of the word "sovereignty" through history and arguing that its meaning "is confused and its uses are various, some of them unworthy, some even destructive of human values").

66. *See, e.g.*, IAN BROWNLIE, PRINCIPLES OF PUBLIC INTERNATIONAL LAW 105–07 (7th ed. 2008) (noting that sovereignty is used liberally by lawyers to describe the "complexity and diversity of the rights, duties, powers, liberties, and immunities of states").

67. For example, the Tenth Amendment reserves all powers (not otherwise delegated in the U.S. Constitution) to the "States respectively, or to the people." U.S. CONST. amend. X.

unhelpful for describing the situation. The closest analogue in international law to this political notion of sovereign will is the principle of self-determination, the right of all peoples to determine for themselves their political destiny. *That* is the norm that was violated during the election.

The election process is the ultimate expression of a people's sovereign will. By illicit interference, the Russians influenced the election to produce the sovereign will of the Russian people (or its government), rather than the sovereign will of the American people. Arguably, Russia was concerned that Clinton would pursue regime change as official U.S. policy and viewed this possibility as an existential threat.[68] The interference substituted one sovereign will for the other as an outcome of the election. Doing so violated the right of the American people to self-determination.

There are several reasons why international lawyers have been unwilling to discuss this incident with the language of self-determination, which is part of a more general hesitation surrounding the legalization of the right of self-determination. First, self-determination is usually invoked as an argument for *constructing* a State (perhaps through secession),[69] but once a State has been created, the legal discourse usually shifts to State sovereignty and the principle of self-determination fades into the background. But that fading away is not legally required; indeed, a people's right to self-determination does not disappear once it succeeds in creating a State to fulfill its self-determination. The concept of State sovereignty does not entirely exhaust the principle of self-determination, which remains an important guiding principle and runs parallel to the legal concept of State sovereignty.

The second problem with invoking self-determination in this context is that the argument presupposes that we can identify, *ex ante*, the sovereign will of the American people, before viewing the results of the election—the process which defines the sovereign will as its ultimate expression. So, for example, a critic might look at the election results and say that the resulting election of Trump was the expression of the American people's self-determination, and there is little empirical evidence to the contrary. That being said, perhaps it is possible to identify the true expression of a people's self-determination by invoking counterfactual thinking, which is commonplace in legal discourse. In the absence of the Russian interference, the election would have proceeded quite differently, suggesting that the

68. ASSESSING RUSSIAN ACTIVITIES, *supra* note 9, at 1 ("Putin most likely wanted to discredit Secretary Clinton because he has publicly blamed her since 2011 for inciting mass protests against his regime in late 2011 and early 2012, and because he holds a grudge for comments he almost certainly saw as disparaging him.").

69. *See* Secession of Quebec, [1998] 2 S.C.R. at 283 (discussing the limits on the right to self-determination when that right would violate the territorial integrity or political unity of the State). For a discussion, see generally MILENA STERIO, THE RIGHT TO SELF-DETERMINATION UNDER INTERNATIONAL LAW: "SELFISTANS," SECESSION, AND THE RULE OF THE GREAT POWERS (2013) (surveying the theory of self-determination and analyzing the right as applied to five locations interested in secession).

actions of Russia distorted and interfered with the American people's right of self-determination.[70]

The third problem is that concluding that Russia violated the American people's right to self-determination might entail that in previous elections it was the United States that violated the right to self-determination when it meddled in the political and electoral process of a foreign nation.[71] But the mere fact that the United States itself may have violated the norm in prior occasions does not necessarily entail that the United States cannot be victimized by similarly illegal conduct or that the activity is not illegal. Widespread noncompliance does not automatically transform the behavior into compliance, the rules of customary international law (via State practice) notwithstanding. More importantly, even if the United States has engaged in such meddling before, it is important to distinguish between political interference in dictatorships and other illiberal systems versus interference in genuinely democratic elections.[72] The former violates the principle of self-determination while the latter does not.[73] Indeed, it should count as a virtue of the self-determination rubric that it helpfully distinguishes between interventions that frustrate democratic self-government and interventions that support it. Furthermore, it is a vice of the blunt tool of State sovereignty that as a legal concept it is incapable of making such crucial distinctions.

Conclusion

We should be clear on specifically how the self-determination legal analysis differs from the sovereignty analysis. Both analyses agree that interference with a foreign political process might be illegal.74 Indeed, as

70. *But see* ASSESSING RUSSIAN ACTIVITIES, *supra* note 9, at i ("We did not make an assessment of the impact that Russian activities had on the outcome of the 2016 election.").

71. *See* Ishaan Tharoor, *The Long History of the U.S. Interfering with Elections Elsewhere*, WASH. POST (Oct. 13, 2016), https://www.washingtonpost.com/news/worldviews/wp/2016/10/13/the-long-history-of-the-u-s-interfering-with-elections-elsewhere/?utm_term=.312a2b7fea1f [https://perma.cc/EPL7-CPYH] (giving examples of U.S. interference in Iran, Chile, and Guatemala among others).

72. Some historical examples of U.S. meddling in foreign political processes arguably involved the frustration of democratic processes in favor of nondemocratic regimes that were viewed as more friendly to U.S. interests.

73. In fact, this is a core difference between the sovereignty and self-determination frameworks; the concept of sovereignty leaves little room for discriminating between political arrangements.

74. For example, the *Tallinn Manual* concludes:

> [T]he matter most clearly within a State's *domaine réservé* appears to be the choice of both the political system and its organization, as these issues lie at the heart of sovereignty. Thus, cyber means that are coercive in nature may not be used to alter or suborn modification of another State's government or social structure.

TALLINN MANUAL 2.0, *supra* note 4, at 315.

long ago as the Nicaragua case, the ICJ concluded that sovereignty entails the "choice of a political, economic, social, and cultural system, and the formulation of foreign policy."[75] What is different is that proceeding under the doctrine of self-determination escapes the formalistic and doctrinal requirements for illegal interventions, including the requirement of coercion.

75. Nicar. v. U.S., 1986 I.C.J. at 107, ¶ 205.

Squinting Through the Pinhole: A Dim View of Human Rights from *Tallinn 2.0*

Dinah PoKempner*

Like the paradoxical task of establishing "law" to govern "war," the *Tallinn Manual* project of describing international law applicable to cyberattack is an exercise in mediating contending impulses. The law must on the one hand provide sufficient specificity and constraint to achieve its purpose—whether that is humanitarian protection or avoidance of easy resort to disproportionate, excessive, or destructive response. Such limits not only enable greater predictability in foreign relations but further the security and normative aims of humane, peaceful, rights-respecting societies. On the other hand, states and their legal advisors often appreciate and seek international rules articulated at a sufficient level of generality and elasticity to preserve room for maneuver and advantage. Beneath the lofty vantage point of legal consensus on a rule may lie anything from slight deviations on the interpretive path to a veritable battlefield. Restatements of the law are more valuable to the extent they get the points of consensus right and shine a strong light on everything else. While the initial *Tallinn Manual* volume on the laws of armed conflict was reasonably successful on this measure, the 2.0 version is less so, and nowhere is this more evident than in its chapter on international human rights law (IHRL).

This essay will evaluate the chapter in view of the *Tallinn Manual 2.0*'s stated objective: furnishing "[s]tate legal advisors charged with providing international law advice to governmental decision makers" with "an objective restatement of the *lex lata*."[1] As a practitioner, I deeply appreciate the pragmatic approach. Unfortunately, the effort fails its own objective, both by approaching international human rights law through the blurry lens of customary international law and in its uneven and debatable account of what actually comprises that body of law. While the editors and authors plainly intend that their audience be mindful of human rights, the fluid and rapidly developing law in this area presents challenges, and so do widening divisions of opinion that are evident between governments, international experts, and civil society on what human rights law requires in the new digital age. This essay will discuss both the *Tallinn Manual* approach and the treatment of specific issues in IHRL. Human rights law applies in both peace and wartime, and to every action of government affecting individuals, so its

---

* General Counsel, Human Rights Watch; Associate Professor, Columbia University. I am grateful to Max Anderson for research assistance; errors are mine alone.

1. TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS 2, 3 (Michael N. Schmitt & Liis Vihul eds., 2017) [hereinafter TALLINN MANUAL 2.0].

omission from the *Manual* would be irresponsible. But to get the law right, the conscientious legal advisor should look elsewhere, and I will make suggestions throughout to that end.

I. The View from Military and National Security Experts on IHRL

A group of legal practitioners, academics, and technical experts were chosen by the editors to constitute International Groups of Experts who by discussion and consensus formulated and drafted rules. In the first round dealing with *jus ad bellum* and *jus in bello*, these persons were mainly experts in international humanitarian law (IHL), as one would expect. But in round 2.0, dealing with public international law in times of peace, the experts were also mainly ex-government or academic lawyers with expertise in military or national security law (with Steven Hill from the North Atlantic Treaty Organization (NATO) as a nonvoting organizational observer), and this perspective informs the text, edited by Michael Schmitt of the United States Naval War College and Liis Vihul then of the NATO Cooperative Cyber Defence Centre of Excellence.[2] Many, though certainly not all, of the well-known experts, contributors, and peer reviewers had also served as advisors to government,[3] and the government of the Netherlands sponsored several rounds of reaction and input to the drafters by governments.[4]

Military and national security lawyers may care deeply about human rights but generally do not develop deep familiarity with IHRL and its constitutive processes—that is more typical of human rights advocates, litigators, academics, and state specialists.[5] Within governments, there is a fair amount of institutional separation: human rights are generally cabined in departments of foreign affairs, and national security matters are dealt with in departments of defense or interior. At the U.N., the substantial human rights apparatus—the Human Rights Council, the Expert Mechanism, the Third Committee—is entirely distinct from the U.N. Office on Drugs and Crime, the Internet Governance Forum, or the Group of Governmental Experts, and despite recent efforts to expose these latter groups to the work of human rights experts, there is still some way to go in integrating human rights expertise.[6] It took years for the United Nations to incorporate human rights

2. *Id.* at xii, xiii, xxii.

3. *See id.* at xii–xviii (listing directors, technical and legal peer reviewers, and legal researchers and their respective institutions).

4. *Id.* at xxvi (describing the Netherlands government's involvement with the drafting process).

5. *See* David Luban, *Military Necessity and the Cultures of Military Law*, 26 LEIDEN J. INT'L L. 315, 315–17 (2013) (describing deep cultural differences between military lawyers and human rights lawyers).

6. For example, since 2012 the U.N. Office on Drugs and Crime—which increasingly invites participation by civil-society organizations, including human rights groups—has begun internalizing international human rights as relevant to its work. *UNODC Intensifies Focus on Human Rights*, U.N. OFF. ON DRUGS & CRIME (May 25, 2012), https://www.unodc.org/unodc/en/frontpage/2012/May/unodc-intensifies-focus-on-human-rights.html

expertise into its counterterrorism bodies, and the most recent report of the Special Rapporteur on Counter-terrorism and Human Rights charts the distance still to be traveled.[7]

Another obstacle to the clear application of IHRL to various government actions in the area of cyberattack is the trend towards blurring the distinction between the law of peacetime, where IHRL fully applies, and the law of armed conflict, where it coexists with IHL and where particular provisions may be subject to derogation or displacement by a more specific law. From its inception in the United States, "war on terror" rhetoric has functioned to obscure the legal regime that governs particular interventions,[8] complicating human rights evaluation. Offensive and defensive functions in cyber operations often merge at the institutional level, also complicating application of human rights law.[9] The issue of when transborder operations are covered by a state's international human rights obligations is deeply contested.[10] In short, institutional obstacles to considering human rights law in the context of cyber operations are considerable for many reasons,

---

[https://perma.cc/X5TB-QJGQ]. Similarly, the Internet Governance Forum, a multistakeholder organization that brings both state representatives and nonstate experts together, recognizes human rights topics as relevant to its mandate. *See, e.g.*, *Human Rights, Freedom of Expression and Free Flow of Information on the Internet*, IGF, http://www.intgovforum.org/cms/component/content/article/121-preparatory-process/1343-human-rights-freedom-of-expression-and-free-flow-of-information-on-the-internet [https://perma.cc/DTQ7-UGYP] (providing an overview of a 2016 meeting session on human rights and free expression on the Internet). By contrast, the U.N. Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security excludes human rights experts and mentions international human rights law as relevant to their concerns only in passing. *See, e.g.*, U.N. Secretary-General, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, ¶ 28, U.N. Doc. A/70/174 (July 22, 2015).

7. *See* Ben Emmerson (Special Rapporteur), *Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism*, U.N. Doc. A/HRC/34/61, at 4, 15–20 (Feb. 21, 2017) (identifying possible reforms of the U.N.'s institutional architecture that would address human rights issues in the counterterrorism context).

8. *See* Kenneth Roth, *Must It Always Be Wartime?*, N.Y. REV. BOOKS (Mar. 9, 2017), http://www.nybooks.com/articles/2017/03/09/must-it-always-be-wartime/ [https://perma.cc/KP2C-6TFV] (noting that "war on terror" rhetoric and other modern aspects of armed conflict serve to blur the lines between war and peace).

9. *See, e.g.*, Ashley Carman, *The NSA Is Merging Its Cyber Offense and Defense Teams*, THE VERGE (Feb. 6, 2016), http://www.theverge.com/2016/2/8/10900234/nsa-offense-defense-nsa21-restructuring [https://perma.cc/4U9Z-DAVW] (explaining that "the [NSA] team that collects information about system vulnerabilities in order to exploit them for espionage purposes will work alongside the team that collects information about vulnerabilities in order to shield U.S. networks from cyberattacks"). *See generally* Gabor Rona & Lauren Aarons, *State Responsibility to Respect, Protect and Fulfill Human Rights Obligations in Cyberspace*, 8 J. NAT'L SEC. L. & POL'Y 503 (2016) (discussing the issues of applying international human rights law to cyberspace).

10. *See* Beth Van Schaack, *The United States' Position on the Extraterritorial Application of Human Rights Obligations: Now Is the Time for Change*, 90 INT'L L. STUD. 20, 21–22 (2014) (outlining the development of legal doctrines surrounding the recognition of human rights in extraterritorial situations).

including the tendency of military and national security perspectives to dominate the field.

Given this institutional separation, the paucity of human rights experts in the ranks of the *Tallinn Manual 2.0* participants at the drafting stage perhaps is unsurprising. But it is regrettable, along with the absence of industry, nonmilitary technicians, or civil-society organizations, given the "multistakeholder" approach that has taken hold in cyber-security projects and that is increasingly evident in other cyberlaw and regulatory processes such as that leading to Brazil's Marco Civil[11] or that of the Internet Governance Forum.[12] Indeed, nongovernmental experts, practitioners, and scholars have for decades provided much of the gas in the engine of human-rights-law mechanisms, be they treaty bodies, courts, review conferences, U.N. or regional procedures, or legislatures, and not only through the supply of relevant facts but through legal analysis and interpretation. One suspects that the framers of the *Tallinn Manual 2.0* process, by limiting exposure of the draft to a broader community of human rights experts and stakeholders, were striving to provide a more statist view[13] of IHRL than normally is on view in scholarship or U.N. publications, but here the framers have missed the mark: IHRL, which operates to bind states to the benefit of ordinary people, is profoundly shaped not just by states, but by the nonstate champions of those beneficiaries. To minimize that perspective guarantees more than a little distortion in the picture of the law.

II. Narrowing the Aperture: Customary International Law of Human Rights

The likely response of the project's coordinators to my observation on the minimal participation of civil society or specialists in IHRL is that a multistakeholder approach may be appropriate when considering the direction human rights law ought to go, but theirs is a project of assessing where it is now, the *lex lata* rather than the *lex ferenda*. While it is true that, like government lawyers, many nongovernmental experts engage in

---

11. Ronaldo Lemos et al., *A Bill of Rights for the Brazilian Internet ("Marco Civil")—A Multistakeholder Policymaking Case*, INST. FOR TECH. & SOC'Y RIO DE JANEIRO ST. U., *available at* https://publixphere.net/i/noc/page/IG_Case_Study_A_Bill_of_Rights_for_the_Brazilian_Internet [https://perma.cc/P9PU-2TVF].

12. JEREMY MALCOM, MULTI-STAKEHOLDER GOVERNANCE AND THE INTERNET GOVERNANCE FORUM 19 (2008). Multistakeholder arrangements are increasingly common in many aspects of Internet governance. *See NoC Study on Internet Governance*, GLOBAL NETWORK INTERNET & SOC'Y RES. CTRS., http://networkofcenters.net/research/internet-governance [https://perma.cc/98YF-MRUM] (examining existing multistakeholder systems in Internet governance).

13. *See, e.g.*, Michael N. Schmitt & Sean Watts, *State* Opinio Juris *and International Humanitarian Law Pluralism*, 91 INT'L L. STUD. 171, 174–75 (2015) (lamenting states ceding control over the content, interpretation, and development of IHL to nonstate experts and civil society, among others).

advocacy in the interests of their clients, practitioners in the field of IHRL generally are familiar with a wide range of state practices in many situations, and how they have been tested by a wide variety of adjudicative bodies. This might have been useful in assessing what is surely the most peculiar aspect of *Tallinn 2.0*, the idea that the *lex lata* of human rights can be discerned from a narrow focus on customary international law.

There are areas of international law with deep bedrock in centuries or many decades of readily discernable customary practice where restatement of customary international law is valuable to the practitioner. International humanitarian law is surely one, and general legal principles of jurisdiction and sovereignty are other areas where custom had a significant history. Resort to custom is critical where treaties are lacking, where treaties have big gaps, or where major players in the field fail to ratify key treaties but confirm that the instruments partially reflect duties they recognize in customary international law.[14]

IHRL is not one of these areas. It emerged from the mire of World War II and the major atrocities of the late-twentieth century, and it is planted thick with treaties. Many of these treaties are quite widely ratified and equipped with treaty bodies that evaluate state reports, generate interpretations of the law, and even determine complaints under optional protocols.[15] The International Covenant on Civil and Political Rights, for example, has 169 states parties and 6 signatories; the International Covenant on Economic, Social, and Cultural Rights has 165 states parties and 5 signatories.[16] These offspring of the Universal Declaration of Human Rights (a core statement correctly identified by *Tallinn 2.0* as reflective of customary law) are often used to explicate the Declaration's rules, making them essential to understanding the current state of the law.[17] Unless you are the legal advisor to the few nations outside this treaty regime, you are much more

14. *See, e.g.*, Michael J. Matheson, *The United States Position on the Relation of Customary International Law to the 1977 Protocols Additional to the 1949 Geneva Conventions*, 2 AM. U. J. INT'L L. & POL'Y 419, 420 (1987).

15. The Office of the High Commissioner for Human Rights lists nine "core" human rights treaties, complete with treaty bodies and optional protocols. *The Core International Human Rights Instruments and Their Monitoring Bodies*, U.N. HUM. RTS. OFF. OF THE HIGH COMMISSIONER, http://www.ohchr.org/EN/ProfessionalInterest/Pages/CoreInstruments.aspx [https://perma.cc/3PNJ-RUCX]. This list does not include closely related bodies of law, such as International Labor Organization treaties; refugee instruments; or minority, indigenous, or tribal rights instruments. *Id.*

16. *Status of Ratification Interactive Dashboard*, U.N. HUM. RTS. OFF. OF THE HIGH COMMISSIONER, http://indicators.ohchr.org/ [https://perma.cc/59PX-NMAP] (last visited May 14, 2017) (information accessable under the "Select a treaty" dropdown list).

17. *See, e.g.*, *International Covenant on Civil and Political Rights*, EQUAL. & HUM. RTS. COMMISSION, https://www.equalityhumanrights.com/en/our-human-rights-work/monitoring-and-promoting-un-treaties/international-covenant-civil-and [https://perma.cc/3ANG-8Y7X] (last updated Nov. 3, 2016) (stating that both the International Covenant on Civil and Political Rights and the International Covenant on Economic, Social, and Cultural Rights give "legal force" to the Universal Declaration of Human Rights).

likely to start here as your reference point than to search for consensus on what states understand as customary obligations.

Most conscientious legal advisors will start their quest to understand IHRL with the treaties to which their states adhere, how they are interpreted by the relevant treaty bodies, and how they are incorporated and understood in their municipal law. To minimize contention at an international level, legal advisors may also wish to know how the norms are understood by the various U.N. expert mechanisms as well as by other states in the context of U.N. bodies. The regional law, commissions, and courts may also be relevant, as well as the municipal law of states parties most affected or involved by the policy decisions at hand. If this sounds like a big endeavor, it is; there has been an explosion of international human rights law, including accountability measures, in the decades since World War II.[18]

Despite the thickness of written law in this area,[19] exploring it can make lawyers from other disciplines uncomfortable. International human rights law feels different, more ideological than many other areas of law—ratifications are plentiful, including from states that show little intention of adhering to the norms they endorse. Treaties and predecessor declarations (not to mention post-treaty diplomatic conference statements, optional protocols, subsequent resolutions, or declarations pertinent to interpretation) tend to be written in a vague, moralistic, hortatory style to achieve the most universal adoption. Reservations of dubious validity are often criticized but seldom result in exclusion from the treaty regime for the same reason.[20] Human rights law does not fit easily into either a transactional or realist view of the world, as member states are guaranteeing rights to those within their own territory and jurisdiction rather than to their treaty partners, making reciprocity a less reliable guide to compliance. Government lawyers often read it narrowly, even with respect to the behavior of foreign states, from concern IHRL might one day hobble their client's discretion beyond the constraints of its own constitutional law. It's hard to measure or achieve compliance under IHRL due to its broad scope and the vast number of governmental and nongovernmental actors engaged—far beyond the military and law enforcement realms. And to top it off, the law is in rapid motion, changing almost constantly through complex processes of advocacy,

18. TALLINN MANUAL 2.0, *supra* note 1, at 179–80. *See generally* Thomas Buergenthal, *The Evolving International Human Rights System*, 100 AM. J. INT'L L. 783 (2006) (discussing the dramatic growth of international human rights law and the mechanisms that have evolved to protect political and civil rights).

19. *See* Başak Çali, *Comparing the Support of the EU and the US for International Human Rights Law Qua International Human Rights Law: Worlds Too Far Apart?*, 13 INT'L J. CONST. L. 901, 902–03 (arguing that the "thickness" of the international human rights regime in the E.U. is responsible for increased support for international human rights law in Europe).

20. *See* Roslyn Moloney, *Incompatible Reservations to Human Rights Treaties: Severability and the Problem of State Consent*, 5 MELB. J. INT'L L. 155, 156–58 (2004) (describing the dilemma of who determines when a reservation is incompatible with the underlying treaty).

adjudication, negotiation, and elaboration, at the national, regional, and international levels.

But factors that make international human rights law a perpetually moving target in treaty form also complicate zeroing in on its customary-law core. The relatively short history of IHRL, coupled with the rapidity of its development, makes it difficult to reference longstanding state practice from a sense of legal obligation, especially in the very new context of transnational cyber operations. While some perceive "instant customary international law" forming from treaty adoption where no contrary norm existed before,[21] others resist the notion there is such law.[22] It is difficult to find consistent state practice and *opinio juris* in an area where state pronouncements and endorsements are thick, while implementation is often thin to lacking. The issue of what counts as state practice or *opinio juris* is deeply contested in IHRL, with some scholars urging greater attention to state declarations than deeds.[23] And when we examine how this body of law relates to matters of national security or espionage, even public pronouncements are thin and various, as the editors correctly note.[24]

Nevertheless, some scholars believe the quest to locate the customary international law of human rights is valuable, either as a way to surface obscured but real practices or to press the claim of its universality against those who attack it on grounds of cultural relativism.[25] This does not seem to be the motivation of the *Tallinn 2.0* Experts, who agreed with one of the sweeping statements of cultural relativism served up by the much-criticized Association of Southeast Asian Nations (ASEAN) Human Rights Declaration,[26] to the effect that "the realisation of human rights must be considered in the regional and national context bearing in mind different

21. *See, e.g.*, Roozbeh (Ruby) B. Baker, *Customary International Law in the 21st Century: Old Challenges and New Debates*, 21 EUR. J. INT'L L. 173, 176–77 (2010) (describing how customary international law is formed and developed); Michael P. Scharf, *Accelerated Formation of Customary International Law*, 20 ILSA J. INT'L & COMP. L. 305, 318–20 (2014) (presenting the ways that treaties can generate customary rules binding on states).

22. *See generally* Jack L. Goldsmith & Eric A. Posner, *A Theory of Customary International Law*, 66 U. CHI. L. REV. 1113 (1999) (arguing that what appear to be rules evidenced by states acting in similar ways from *opinio juris* are better understood as a coincidences of interest or successful coercion).

23. *See, e.g.*, Samuel Estreicher, *Rethinking the Binding Effect of Customary International Law*, 44 VA. J. INT'L L. 5, 6 (2003).

24. TALLINN MANUAL 2.0, *supra* note 1, at 179.

25. *See, e.g.*, Ralph Wilde, Address at the University of Texas Law Review Symposium: Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Feb. 7, 2017).

26. *See, e.g.*, *ICJ Condemns Fatally Flawed ASEAN Human Rights Declaration*, INT'L COMM'N OF JURISTS (Nov. 19, 2012), https://www.icj.org/icj-condemns-fatally-flawed-asean-human-rights-declaration/ [https://perma.cc/JD44-NJUB] (criticizing the ASEAN's Human Rights Declaration as detrimental to human rights).

political, economic, legal, social, cultural, historical and religious backgrounds."[27]

What are we to make of the inclusion of this chestnut of "Asian values" discourse?[28] Unfamiliarity or disagreement with the universalist nature of human rights law? There is certainly a theme running through the discussions that IHRL is a mainly contractual affair—no natural law discourse here. Perhaps it is a misguided attempt to make the *Manual* more appealing as a desk book to ASEAN governments? The first *Tallinn Manual* has been criticized as a project closely affiliated with NATO.[29] The danger with a manual that aspires to universal adoption is that it will be read as a prestigious invitation to radically bend the interpretation of permissible limitations on rights to fit whatever governments claim are their own unique national circumstances—an eviscerating approach to IHRL.

This is not just a quibble, as the chapter is inconsistent with how it treats regional law concepts, given its project of locating near-universal custom. Another regional doctrine recycled as a generalization is approving reference to the European law concept of a state "margin of appreciation" in applying rights law,[30] a concept that has been criticized by the U.N. human rights bodies.[31] While the Experts worry about the very European nature of proportionality analysis in evaluating limitations on the right to privacy, they are eager to adopt a European perspective on personally identifying information and speculate on how that may be an elevated category of data worthy of heightened privacy protection. On the other hand, they ultimately reject, but give lots of space to discussing, the doctrine of "reasonable expectation of [privacy],"[32] a concept rapidly approaching obsolescence even in the United States.[33]

---

27. TALLINN MANUAL 2.0, *supra* note 1, at 180.

28. *See generally* Xiaorong Li, *"Asian Values" and the Universality of Human Rights*, 16 PHIL. & PUB. POL'Y Q. 18 (1996) (analyzing the interaction between Asian values and international human rights).

29. *See* Kristen Eichensehr, Book Review, 108 AM. J. INT'L L. 585, 585 (2014) (reviewing TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE (Michael N. Schmitt ed., 2013)) (recognizing that the NATO-centric perspective of *Tallinn Manual 1.0* may draw criticism from non-NATO countries).

30. *See* TALLINN MANUAL 2.0, *supra* note 1, at 180, 205 (indicating that the International Group of Experts agrees that states enjoy a "margin of appreciation" in limiting human rights obligations).

31. *See, e.g.*, U.N. Human Rights Comm'n, International Covenant on Civil and Political Rights, U.N. Doc. CCPR/C/GC/34, at 8–9 (Sept. 12, 2011) (rejecting the "margin of appreciation" analysis when evaluating limitations on freedom of expression).

32. *See* TALLINN MANUAL 2.0, *supra* note 1, at 191 (noting the Experts' discussion of, but lack of agreement on, a reasonable-expectation-of-privacy standard for the right to privacy under customary international law).

33. *See* United States v. Jones, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring) (suggesting that the reasonable-expectation-of-privacy doctrine may need reconsideration).

Yet even where there is scholarly enthusiasm for discovering the customary international law of human rights, there is little consensus on what makes the grade, so texts and restatements tend to describe the ambit conservatively. *Tallinn 2.0* is no exception to the conservative approach. The Experts caution "it is often unclear as to whether certain human rights reflected in treaty law have crystallised as rules of customary law,"[34] and they note that the congruence of multiple treaties and case law on a particular point "may support, but does not necessarily do so definitively, a conclusion that customary international law exists to that effect."[35] In effect, the editors and their Experts have chosen the narrowest pinhole through which to view this subject.

III. A Little Consensus

Having chosen this limited aperture of customary law, the Experts predictably find it difficult to see much detail to agree on. It is hard to say whether this is the unfortunate result of their terms of reference or the end towards which the terms were designed. IHRL, in their view, is a hazy, "[s]pecialized" regime that does not answer many questions.[36] So it is all the more to be welcomed that some areas of agreement and real progress were noted.

Although the chapter begins with a qualified statement—"[*i*]*t is widely accepted that many* of the international human rights that individuals enjoy 'offline' are also protected 'online'"[37]—Rule 35 correctly drops the hedging language I have italicized and states it in the declarative form that has been unanimously and repeatedly adopted at the U.N. Human Rights Council and the General Assembly,[38] to wit, "[i]ndividuals enjoy the same international human rights with respect to cyber-related activities that they otherwise enjoy."[39] This is an important starting point for inclusion of human rights considerations in a wide variety of cyber-security problems, as well as examination of whether there is any justification for limiting rights online to a greater degree than offline, a practice noted and criticized by the Special

34. TALLINN MANUAL 2.0, *supra* note 1, at 179.

35. *Id.* at 180.

36. *Id.* at 177.

37. *Id.* at 179 (emphasis added).

38. G.A. Res. 69/166, The Right to Privacy in the Digital Age, at 3 (Dec. 18, 2014); G.A. Res. 68/167, at 2 (Dec. 18, 2013); Human Rights Council Res. 32/13, U.N. Doc. A/HRC/RES/32/13, at 3 (July 1, 2016); Human Rights Council Res. 26/13, U.N. Doc. A/HRC/RES/26/13, at 2 (June 26, 2014); Gulnara Iskakova (Rapporteur), Rep. of the Human Rights Council on its Twentieth Session, U.N. Doc. A/HRC/20/2, at 23 (Aug. 3, 2012).

39. TALLINN MANUAL 2.0, *supra* note 1, at 187 (Rule 35).

Rapporteur on the promotion and protection of the right to freedom of opinion and expression,[40] though largely unaddressed by the *Manual*.

It was also heartening to see that the Experts agreed that both IHRL and IHL apply to cyber-related activities in the context of an armed conflict, although the precise interplay was not explored and viewed as "unsettled,"[41] which is accurate, and perhaps an understatement. The Experts also agree that cybercriminals are entitled to due process[42] and that human rights law entails an obligation, not only for the state to respect rights, but to protect the individual from third party violations of rights.[43] All uncontroversial, apple pie and motherhood stuff.

More unusual was express recognition that the right to freedom of opinion is distinct from freedom of expression and is not subject to restriction.[44] It would have been better to note that the restriction includes both limitation and derogation, and that the same is true of freedom of belief,[45] which is distinct from freedom to manifest one's religion.[46] Unfortunately, the illustration of an interference, online intimidation, or harassment of an individual, conducted on the basis of that person's views,[47] is likely to cause confusion because without further definition and an objective standard, this may suggest merely criticism or vocal opposition—both activities that are covered by freedom of expression. I also wished that the authors had explored the interaction of these rights with limitable rights, as when restrictions on privacy, speech, or access to information are so severe as to interfere with our ability to form and hold opinions and beliefs, a concept that finds reflection in doctrines of right of personality.[48]

It was also striking to read "the Experts were aware of no *opinio juris* suggesting that states consider espionage *per se* to fall beyond the bounds of their international human-rights-law obligations concerning the right to privacy."[49] I am not sure why they framed this observation only with respect

40. Frank La Rue (Special Rapporteur), Promotion and Protection of the Right to Freedom of Opinion and Expression, U.N. Doc. A/66/290 (Aug. 10, 2011), http://ap.ohchr.org/documents/dpage_e.aspx?si=A/66/290 [https://perma.cc/WH8F-TB2H].

41. *Id.* at 181.

42. *Id.* at 193.

43. *Id.* at 196–98 (Rule 36).

44. *Id.* at 188.

45. G.A. Res. 2200A, International Covenant on Civil and Political Rights art. 18 (Dec. 16, 1966) [hereinafter ICCPR].

46. *Id.* art. 18.

47. TALLINN MANUAL 2.0, *supra* note 1, at 189.

48. *See, e.g.*, Bart van der Sloot, *Privacy as Personality Right: Why the ECtHR's Focus on Ulterior Interests Might Prove Indispensible in the Age of "Big Data"*, 31 UTRECHT J. INT'L & EUR. L. 25, 34–35 (2015) (discussing the right to personal development as found in the Universal Declaration on Human Rights).

49. TALLINN MANUAL 2.0, *supra* note 1, at 193.

to the right to privacy, as espionage affects many other rights as well, but I am glad they got that far.

This recognition that IHRL is applicable to espionage, however, does not lead to many conclusions, given the lack of consensus on extraterritorial obligation. The Experts generally agree that customary IHRL applies beyond a state's borders where it exercises physical "power or effective control" over territory or persons, another welcome bit of progress given the historical U.S. reluctance to even acknowledge extraterritorial obligation under *treaty* law.[50] But the Experts do not agree on whether there is a customary rule that "power or effective control" can be exercised by *virtual* means across borders.[51] So we are thrown back on treaty law again, where all the Experts can agree on is that Article 2(1) of the ICCPR "governs the treaty's extraterritorial applicability, or lack thereof."[52] Here I picture my hypothetical legal advisor thinking, "Gee, thanks guys" (and yes, the Experts are overwhelmingly guys).

IV. A Lot of Contention

As the above illustrates, consensus often stops at the obvious and does not go very deep. But there is a lot of contention—some of it interesting and some of it disturbing—as it pertains to matters that have received a good deal of attention in the law. This section focuses on several issues where the Experts have difficulty agreeing on what most human rights law experts would consider good candidates for customary principles.

The right to privacy, predictably, gives the Experts a lot of trouble. Here one cannot escape the perception that the discussion often tracks justifications of U.S. mass-surveillance practices exposed by Edward Snowden. Though privacy law encompasses a wide range of topics relating to a person's autonomy, identity, and association that are surely relevant to issues of hacking, doxxing, and similar intrusive activities, the Experts focused tightly on a few specific matters relating to communications privacy and personal data in what reads like a topic dominated by the consideration of mass-surveillance practices among the Five Eyes.[53]

---

50. *Id.* at 184. Despite the recommendation of then-Legal Adviser Harold Koh, the U.S. maintained the position that the International Covenant on Civil and Political Rights imposes no obligation outside a state party's territory. Marko Milanovic, *Harold Koh's Legal Opinions on the US Position on the Extraterritorial Application of Human Rights Treaties*, EJIL: TALK! (Mar. 7, 2014), https://www.ejiltalk.org/harold-kohs-legal-opinions-on-the-us-position-on-the-extraterritorial-application-of-human-rights-treaties [https://perma.cc/W73L-SSJL].

51. TALLINN MANUAL 2.0, *supra* note 1, at 185–86.

52. *Id.* at 186.

53. *See* TALLINN MANUAL 2.0, *supra* note 1, at 189–91 (recounting the Experts' views on privacy in e-mail communications and their inability to agree on a precise definition of "personal data"). The Five Eyes is the shorthand name for the participant countries—Britain, the U.S., Australia, New Zealand, and Canada—in an intelligence-gathering agreement that has been in place since World War II. Paul Farrell, *History of 5-Eyes—Explainer*, GUARDIAN (Dec. 2, 2013)

It will surprise quite a few privacy law experts to hear that the *Tallinn* Experts could not agree that privacy is implicated by machine inspection of communications until the point of human review. They also had trouble agreeing on a privacy intrusion from "mere collection" of communications.[54] (Nonlawyers, and for that matter, small children, might have a hard time agreeing that if, uninvited, I stick my hand into your mailbox and stuff your letters into my purse, no intrusion on privacy has occurred.) No international law, or any practice, is cited to support the proposition of no rights interference in either situation, though there is quite a bit of support for collection or storing as a privacy intrusion, helpfully set out at footnote 420 in the *Manual*.[55]

If one were to look for state practice in support of the "no intrusion" view, perhaps the contention of the U.S. government on mass-surveillance collection, or some of the recently minted European surveillance laws under legal challenge, would provide support.[56] An alternate perspective might be whether any of these states would excuse or exonerate foreign espionage or theft of state secrets simply because the agents merely unleashed technology to sort and steal the data but can show no one got around to reading the trove. The conclusion that the matter is still too contested to be customary international law is probably defensible, though again, this does not really help the legal advisor with *lex lata* given the lawsuits and pronouncements already out under various international treaties.[57]

Given the lack of agreement on whether a state's collection or algorithmic sorting implicates privacy, there's no surprise that the Experts divided on the issue of metadata, which is often what the algorithm "reads" and uses for collection. Here the *Manual* again swims into uncharted water, trying (without any supporting citation) to stuff the issue of metadata into the somewhat separate legal area of data protection of personally identifiable information, or as they style it, "personal data."[58] This much they agree on: the right to privacy is implicated if the metadata is unambiguously "personal

---

https://www.theguardian.com/world/2013/dec/02/history-of-5-eyes-explainer [https://perma.cc/6E93-BXDU].

54. TALLINN MANUAL 2.0, *supra* note 1, at 190.

55. *Id.* at 190 n.420.

56. Bruce Schneier, *Why the NSA's Defense of Mass Data Collection Makes No Sense*, THE ATLANTIC (Oct. 21, 2013), https://www.theatlantic.com/politics/archive/2013/10/why-the-nsas-defense-of-mass-data-collection-makes-no-sense/280715/ [https://perma.cc/MXN3-A3LX]; James Vincent, *Legal Challenge Against UK's Sweeping Surveillance Laws Quickly Crowdfunded*, THE VERGE (Jan. 10, 2017), http://www.theverge.com/2017/1/10/14222990/uk-surveillance-liberty-legal-challenge-crowdfunding-campaign [https://perma.cc/KR8Z-JHPX].

57. *See* Leander v. Sweden, 9 Eur. Ct. H.R. 433, ¶ 48 (1987) (holding that storing information alone can interfere with the right to privacy).

58. *See* TALLINN MANUAL 2.0, *supra* note 1, at 191–92 (agreeing that "the right to privacy generally protects the personal data of individuals" and that "metadata qualifying as personal data is protected").

data" (undefined). Other metadata they cannot agree on, giving the example of IMAP or POP3 protocol signifiers as unlikely to implicate privacy concerns.

The problem here is that the Experts are missing the main privacy concern with metadata. The issue is not whether a particular bit of metadata is revelatory of some private fact—the way personally identifying information is—but that the aggregation and analysis of metadata (even IMAP or POP3 protocols) can reveal more than even the substance of a communication about someone's private life.[59] Each bit of metadata is part of a mosaic that can map a story, even if its use is only to eliminate other possibilities. The e-mail address of a politician may be widely known and not that sensitive. The politician's correspondence may be very guarded or even encrypted. But a metadata trail showing regular midnight perambulations and cash withdrawals around a foreign embassy, or use of the opposition leader's wife's computer connection, might create quite a different impression. In any event, the Experts' discussion here seems entirely untethered from law, as the only case cited supports the proposition that all metadata is protected.[60]

Another rather shocking pronouncement is that the Experts did not agree "on whether the obligation to provide remedies to victims of international human rights law violations is of a customary nature."[61] This statement then cites U.N. General Assembly resolutions and U.N. guidelines in support of the obligation to provide a remedy, though for some reason not treaty paragraphs that support the obligation as well.[62] Such a conclusion, which is not only unsupported but plainly inconsistent with the development of IHRL over the last half-century,[63] forecloses many other interesting discussions, including whether states have a duty to remove obstacles to challenges to

59. *Privacy Rights, Metadata, and Aggregation*, CAN. CIV. LIBERTIES ASS'N (May 13, 2015), https://ccla.org/privacy-rights-metadata-and-aggregation/ [https://perma.cc/SBY6-8AEW]; *see* Dahlia Lithwick & Steve Vladeck, *Taking the "Meh" out of Metadata*, SLATE (Nov. 22, 2013), http://www.slate.com/articles/news_and_politics/jurisprudence/2013/11/nsa_and_metadata_how_the_government_can_spy_on_your_health_political_beliefs.html [https://perma.cc/U43X-H627] (describing conclusions that can be drawn from data aggregation).

60. *See* TALLINN MANUAL 2.0, *supra* note 1, at 192 (citing Malone v. United Kingdom, 82 Eur. Ct. H.R. (ser. A) ¶ 84 (1984)).

61. *Id.* at 200.

62. *Id.* at 200 nn.446–47.

63. For two guides to the multitude of international instruments and declarations recognizing the many aspects of the right to a remedy, see generally INT'L COMM'N OF JURISTS, THE RIGHT TO A REMEDY AND TO REPARATION FOR GROSS HUMAN RIGHTS VIOLATIONS: A PRACTITIONER'S GUIDE (2006), https://www.icj.org/wp-content/uploads/2012/08/right-to-remedy-and-reparations-practitioners-guide-2006-eng.pdf [https://perma.cc/DH6E-EXUP]; Theo van Boven, *The United Nations Basic Principles and Guidelines on the Right to a Remedy and Reparation for Victims of Gross Violations of International Human Rights Law and Serious Violations of International Humanitarian Law*, U.N. AUDIOVISUAL LIBR. OF INT'L L. (2010), http://legal.un.org/avl/pdf/ha/ga_60-147/ga_60-147_e.pdf [https://perma.cc/ZQD4-U4H8].

surveillance practices in courts, or a duty to disclose when evidence used at trial is procured through intelligence surveillance, or a duty to provide adequate information on surveillance practices to legislative or other bodies or the public so that it is possible to discern if violations have occurred and remedies are in order. In fact, the *Manual* explicitly rejects the idea that oversight bodies are somehow required to protect rights in this very opaque area where national security and public order interests demand a high degree of secrecy—an idea it frames simplistically as a prospective remedy for hypothetical abuse, eliding the very difficult issues that make review and redress through other means so difficult in this area.[64]

But perhaps the most disturbing lack of consensus was the omission of proportionality from the rule regarding justifiable limitations on rights, leaving only the criteria that such limitations must be lawful, necessary, and not discriminatory. Proportionality is a bedrock principle of IHRL, just as it is in IHL.[65] To make things worse, the Experts read proportionality as highly distinct from necessity,[66] misunderstanding they are closely related concepts.[67] When a restriction is necessary, it is not only useful or relevant

---

64. *See* TALLINN MANUAL 2.0, *supra* note 1, at 201 ("[*E*]*x ante* preventive monitoring measures far exceed the requirements of current customary international human rights law.").

65. Proportionality appears in two contexts in IHRL. The first is the limitation of derogation of rights "to the extent strictly required by the exigencies of the situation . . . ." International Covenant on Civil and Political Rights art. 4, Mar. 23, 1976, S. EXEC. DOC. E, 95-2, 99 U.N.T.S. 171; U.N. Office of the High Comm'r for Human Rights, Derogations During a State of Emergency, ¶ 4, U.N. Doc. CCPR/C/21/Rev.1/Add.11 (Aug. 31, 2001). The second is proportionality in permissible restriction of rights more generally, often expressed through the condition that restrictions must be "necessary." International Covenant on Civil and Political Rights art. 19, Mar. 23, 1976, S. EXEC. DOC. E, 95-2, 99 U.N.T.S. 171; U.N. Human Rights Comm'n, The Nature of the General Legal Obligation Imposed on States Parties to the Covenant, ¶ 6, U.N. Doc. CCPR/C/21/Rev.1/Add.13 (May 26, 2004). For discussion of the "principle of proportionality" as an overarching feature of many national constitutions and regional human rights instruments, see generally AHARON BARAK, PROPORTIONALITY: CONSTITUTIONAL RIGHTS AND THEIR LIMITATIONS (2012); Kai Moller, *Proportionality: Challenging the Critics*, 10 INT'L J. CONST. L. 709 (2012).

66. *See* TALLINN MANUAL 2.0, *supra* note 1, at 205 (noting that the Experts emphasized that necessity alone is not sufficient to justify limiting obligations under international human rights law); *id.* at 348 (treating "necessary" and "proportionally" as distinct requirements to justify state actions taken in self-defense).

67. The term "necessary," like the term "arbitrary," is indicative of a form of proportionality analysis. *See* Marko Milanovic, *Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age*, 56 HARV. INT'L L.J. 81, 133 (2015) (noting that the Human Rights Committee and the European Court have read "necessary" to include a measure of whether the interference was proportional to achieving a legitimate aim). The principle of proportionality, which first emerged in German constitutional law, is generally stated as having several related parts: consideration of whether a measure is adequate to reach an end, whether it is "necessary" in the sense of least-restrictive, and whether even if the restriction is both adequate and necessary, it conveys greater benefit than harm in the sense of undermining rights. *See, e.g.*, Hiroshi Nishihara, *Constitutional Meaning of the Proportionality Principle in the Context of the Surveillance State*, 26 WASEDA BULL. COMP. L. 1, 4–5 (2008). Elements of this doctrine are found in many constitutional systems and reflected also in the U.N. Human Rights Committee's interpretation of the term. *See, e.g.*, U.N. Human Rights Comm'n, Freedoms of Opinion and Expression, ¶¶ 33–34, U.N. Doc.

to addressing a threat, but actually required to address a "pressing social need."[68] In this way, proportionality analysis begins, and the question of whether there are less restrictive means to the same end quickly follows.[69] Proportionality adds another layer of nuance in that it requires consideration of the overall impact on rights in deciding whether even a necessary restriction can be justified at all—where a measure, even if the only means available to protect a specific public interest, so undermines the essence of rights that the harm outweighs the specific benefit it can achieve.[70] The only support for this gaping omission is citation to U.S. objections to proportionality language in the UNGA resolution on the right to privacy in the digital age, no doubt motivated by the issue of mass surveillance. But here a very obvious question arises: Given the persistent objector rule, so carefully followed by the U.S. government,[71] why would U.S. objection defeat recognition of the customary nature of such a widely recognized standard?[72]

Even worse, the argument that proportionality has not matured into a norm of customary international law is supported by pointing to patently unlawful state practice, in particular "the practice of various [s]tates of imposing limitations . . . that, while possibly advancing a legitimate state purpose, appear to be a greater infringement on human rights than justified by that need."[73] It is difficult to understand why the editors include an obvious (and all too common) rights violation as a way of showing the lack

---

CCPR/C/GC/34 (Sept. 12, 2011) (discussing the limitations of what can be considered "necessary" regarding proportionality considerations); U.N. Human Rights Comm'n, *supra* note 65, ¶ 6 ("Where such restrictions are made, states must demonstrate their necessity and only take such measures as are proportionate to the pursuance of legitimate aims in order to ensure continuous and effective protection of Covenant rights. . . . In no case may the restrictions be applied or invoked in a manner that would impair the essence of a Covenant right.").

68. Handyside v. United Kingdom, 1 Eur. Ct. H.R. 737, ¶ 5 (1976).

69. *See, e.g.*, Office of the High Comm'r for Human Rights, *Freedom of Movement*, ¶ 14, U.N. Doc. CCPR/C/21/Rev.1/Add.9 (1999) (requiring that restrictions on the individual freedom of movement that is enshrined in the International Covenant on Civil and Political Rights "conform to the principle of proportionality").

70. *Id.*; *see also* Frank La Rue (Special Rapporteur), *Promotion and Protection of the Right to Freedom of Opinion and Expression*, ¶ 79, U.N. Doc. A/HRC/14/23 (Apr. 20, 2010) (requiring that a contemplated restriction on freedom of expression "not undermine or jeopardize the essence" of that freedom).

71. Beth Van Schaak, *The United States' Position on the Extraterritorial Application of Human Rights Obligations: Now is the Time for Change*, 90 INT'L L. STUD. 20, 22–23 (2014).

72. One reason might simply be that the U.S. recognizes proportionality analysis in many other rights contexts, for example, as a state party to the ICCPR and its guarantee of free expression. *See* ICCPR, *supra* note 45, art. 19.

73. TALLINN MANUAL 2.0, *supra* note 1, at 204–05.

of consistent practice, when such violations are regularly denounced by many states,[74] even while others frequently resort to them.[75]

By this standard, there is no customary international law of human rights. No one considers that laws against murder fail some rule of recognition or are not considered real and binding laws because people violate them with some frequency. There is much scholarly contention about the right way to judge both state practice and *opinio juris* in the area of IHRL[76] and whether actions such as statements and endorsements made at the U.N. and other international fora, or condemnation of other states' practices, or incorporation of rights into constitutions and municipal law, or employment of human rights consideration in various policy processes, count. But this much is clear: measuring the existence of customary international law of human rights by the yardstick of state violations is an extremist approach.

The problem of what counts as state practice and *opinio juris* surfaces again in the discussion of extraterritoriality of obligation in the context of surveillance. While there was agreement that espionage is not per se exempt from IHRL, the Experts also decided "there is little evidence that when states conduct signals intelligence programmes directed at foreigners on foreign territory, they consider that their activities implicate the international human right to privacy."[77] This is no doubt true; every country seems to spy on foreigners with gay abandon, according to their means. But no country looks complacently upon other countries spying on their population, from within or outside their borders. Such behavior often incurs condemnation and

74. *See, e.g.*, Human Rights Council, Rep. of the Working Group on the Universal Periodic Review, Belarus, at 5–9, U.N. Doc. A/HRC/30/3 (July 13, 2015) (recording statements of concern by at least six countries on Belarus's ongoing violations of its citizens' freedom of the press, assembly, and expression); Human Rights Council, Rep. of the Working Group on the Universal Periodic Review, Bahrain, at 6–7, 10–11, 13, U.N. Doc. A/HRC/21/6 (July 6, 2012) (recording statements of concern by at least ten countries as to Bahrain's ill-treatment of protestors).

75. *See, e.g.*, Human Rights Council, Summary Prepared by the Office of the High Commissioner for Human Rights in Accordance with Paragraph 5 of the Annex to Human Rights Council Resolution 16/21, Russian Federation, at 4, U.N. Doc. A/HRC/WG.6/16/RUS/3 (Jan. 28, 2013) (reporting allegations of torture and ill-treatment of prisoners by the Russian police and security services); Human Rights Council, Summary Prepared by the Office of the High Commissioner for Human Rights in Accordance with Paragraph 5 of the Annex to Human Rights Council Resolution 16/21, Pakistan, at 4, U.N. Doc. A/HRC/WG.6/14/PAK/3 (July 26, 2012) (noting Pakistan's failure to effectively implement laws protecting women from violence).

76. *See* Scharf, *supra* note 21, at 313–29 (reviewing the scholarly debate over the extent to which customary international law consists of general state practice and states' attitudes regarding certain practices); *see also* Vojin Dimitrijevic, *Customary Law as an Instrument for the Protection of Human Rights* 5 (Istituto Per Gli Studi Di Politica, Working Paper No. 7, 2006) (summarizing the debate on international custom as a source of international law to be "determining the proportion of the influence on the existence of the customary rule of consistent practice, or of *opinio juris*, respectively").

77. TALLINN MANUAL 2.0, *supra* note 1, at 185.

sometimes sanction.[78] So what is more reflective of state attitudes in this area—gay abandon or condemnation? If we think that states generally have an obligation to protect the human rights of their populations and that member states of the United Nations are obliged to *cooperate with each other* in promoting and encouraging respect for human rights,[79] it seems a stretch to infer a general state of legal acquiescence from the admittedly widespread but usually clandestine and often-condemned practice of transborder surveillance. Such a conclusion seems even more unlikely in a world where even domestic Internet communications may route across frontiers.

V. Methodological Opacity

The demerits of a focus on customary international law of human rights and the many failures to achieve consensus might be somewhat redeemed if we knew more about who is propounding which position and based on what sources. That, at least, would have directed bright light on the legal debate and given hints as to where the law might be going. But while the *Manual* highlights some interesting discussions, it hides the proponents and often the bases for their arguments—what we get is more like a snapshot of the dance floor with the dancers in silhouette. Even without identifying particular scholars (though why scholars should seek anonymity in this exercise is unclear), evaluating the conversation would be easier if objections were only from one national vantage point, or where a majority view was reflective of a particular regional legal culture. Legal support for many of the contentions in the *Manual* is spotty and sometimes absent even for majority views. Since this work is neither to be taken as one scholar's treatise, nor reflective of one institution, the lack of attribution and support impairs its credibility.

Another obscurity is why certain rights are discussed and others not, and why certain issues are included but others not. For example, since the Experts view "mere" collection of someone's communications as not implicating privacy, they do not bother to discuss the lawful scope of data retention—one of the most urgent issues in digital human rights, as governments assert mandatory retention authority, manufacturers convert the physical world into smart surveillance devices, and courts continue to express alarm. Another topic not dealt with at all in the IHRL chapter is the lawfulness of encryption,

---

78. *See, e.g.*, Alissa J. Rubin, *French Condemn Surveillance by N.S.A.*, N.Y. TIMES (Oct. 21, 2013), http://www.nytimes.com/2013/10/22/world/europe/new-report-of-nsa-spying-angers-france.html [https://perma.cc/4V3W-SE5F] (reporting why the French government castigated the U.S. for "carrying out extensive electronic eavesdropping within France"); David E. Sanger, *Obama Strikes Back at Russia for Election Hacking*, N.Y. TIMES (Dec. 29, 2016), https://www.nytimes.com/2016/12/29/us/politics/russia-election-hacking-sanctions.html [https://perma.cc/S3XQ-47AM] (reporting that the Obama Administration responded to Russia's efforts to influence the 2016 U.S. elections through cyberspace by imposing sanctions on its two leading intelligence services and expelling thirty-five Russian nationals from the U.S.).

79. U.N. Charter art. 1, ¶ 3.

one of the few means individuals have to protect against privacy intrusion and a host of other rights violations, though proposals and laws to make strong encryption unlawful proliferate and the human rights and technical communities express grave alarm.[80] As noted above, the prospect of dissensus on customary international law did not cause the editors to excise many other discussions, so it is hard to see why these important topics are missing.

Given the prospect of finding little established custom to agree on in this area, the *Tallinn* Experts might have chosen to be forward-looking and put a few more unsettled issues on display. Many of the greatest challenges in applying human rights to issues of cyberattack are yet to come. Issues of human rights and artificial intelligence capabilities of means of surveillance, analysis or attack, or the Internet of Things as a target or instrumentality of attack, raise large rights implications that will have to be explored by others, and are likely to confront the legal advisor soon. There are less futuristic concerns that might have gotten more attention, particularly the nature of Internet access to the enjoyment and exercise of rights. Unfortunately, the Experts dismissed as insufficiently established in custom both a right to anonymity and a right to Internet access even while acknowledging these might be essential to the enjoyment of other rights.[81] Such an approach is sensible only under a narrow, scholastic vision of what qualifies as customary international law. When one considers that a right to water is widely recognized because it is implied by other established rights, the justification for this approach becomes questionable.

VI. A Better Approach

What is the legal advisor to do in an era where many pillars of human protection—from the prohibition against torture to the shelter of refugees—seem as under attack as the cyber-infrastructure? The partial and disputable account of customary IHRL in this chapter will not be great help, and to be fair, the *Manual* itself frequently turns the conversation to other sources. My initial recommendation is to look first to treaty obligations and then more widely at international interpretation of rights from the most experienced states and practitioners in the international-, regional-, and state-level

80. AMNESTY INT'L, ENCRYPTION: A MATTER OF HUMAN RIGHTS 12–13 (2016), *available at* https://www.amnestyusa.org/sites/default/files/encryption_-_a_matter_of_human_rights_-_pol_40-3682-2016.pdf [https://perma.cc/AMZ6-6TL8] (decrying several countries' efforts to ban or restrict encryption and the resulting impact on human rights); DANIEL CASTRO & ALAN MCQUINN, UNLOCKING ENCRYPTION: INFORMATION SECURITY AND THE RULE OF LAW 3 (2016), *available at* http://www2.itif.org/2016-unlocking-encryption.pdf?_ga=1.268177294.1861050019.1489516139 [https://perma.cc/5S4X-NA49] (criticizing limitations on encryption as ineffective against terrorism and harmful towards average citizens).

81. *See* TALLINN MANUAL 2.0, *supra* note 1, at 194 (acknowledging that international law has not coalesced on a right to anonymity); *id.* at 13 (recognizing states' sovereign right to disconnect from the Internet).

systems. But I would counsel the legal advisor to consider a few other things as well.

First, actions in the area of human rights are subject to review and scrutiny, not only in the domestic system and from a wide range of advocates and litigants, but also and increasingly internationally. Your duty is to advise your client not just on what it can get away with, but how that action may be received, and not just domestically. To that end, do not be afraid to consult with other departments of government, as well as those with expertise outside of government, even if you think they will disagree. Rehearse your options before the need arises and revisit them, as this law changes quickly. Test the legality of any proposed action *by* your state as though it were directed *against* your state; that exercise helps clarify what principles your government stands for, even in the absence of more direct reciprocity in IHRL. And finally, ask: Will this action, even if justifiable under IHRL, set a potentially damaging precedent either for my state or other nations or will it wind up weakening the foundations of human rights that all democratic societies stand on? Your obligation is not only to the *lex lata*, but to the future as well.

* * *

Beyond Self-Defense and Countermeasures: A Critical Assessment of the *Tallinn Manual*'s Conception of Necessity

Christian Schaller*

Introduction

Much has been written by scholars and practitioners about how the right to self-defense and the law of countermeasures can be applied to combat different threats in cyberspace. It is therefore no surprise that *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* places special emphasis on these concepts.[1] Another possible remedy for responding to serious cyber incidents, which has not attracted much attention so far, is the plea of necessity as outlined in Rule 26 of *Tallinn Manual 2.0*. At first glance, Rule 26 and the seven pages of commentary by which it is accompanied convey a fairly clear and convincing image of necessity in the cyber context. But some doubts remain. The present essay questions, in particular, whether the specific conception of necessity embodied in *Tallinn Manual 2.0* is really an "objective restatement of the *lex lata*."[2] Moreover, it will be shown that the interpretation of Rule 26 is not as uncontroversial as it may appear when reading the relevant passages in the *Manual*. The critique voiced in this essay is based on concerns that the plea of necessity is particularly susceptible to abuse and that an excessive invocation in response to cyber incidents could increase the risk of misperception, escalation, and conflict.

First of all, it needs to be set out in which situations the plea of necessity may become relevant at all. For this purpose it is useful to briefly delineate the scope and limits of the concepts of self-defense and countermeasures. A State facing a cyber operation that constitutes an armed attack can exercise its inherent right to self-defense as laid down in Article 51 of the U.N. Charter, irrespective of whether the attack has been carried out by another State or a non-State actor.[3] In most cases, however, the threshold of an armed

* Dr. iur., Deputy Head Global Issues, German Institute for International and Security Affairs (Stiftung Wissenschaft und Politik, SWP), Berlin (christian.schaller@swp-berlin.org).

1. TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS 111–34, 339–56 (Michael N. Schmitt & Liis Vihul eds., 2017) [hereinafter TALLINN MANUAL 2.0] (stating Rules 20–25, which relate to countermeasures, and 71–75, which relate to self-defense).

2. All rules contained in the *Manual* were adopted by consensus and are regarded by the authors as reflecting customary international law (unless expressly referencing a treaty) as applied in the cyber context. *Id.* at 3–4.

3. U.N. Charter art. 51, 1st sentence (recognizing the "inherent right of individual or collective self-defense" of United Nations members faced with an armed attack and containing no language

attack will not be crossed. Malicious cyber operations of a lower intensity may be repelled with active cyber defenses short of the use of force, which could be permitted under the law of countermeasures. Countermeasures are an instrument to induce a State that is responsible for an internationally wrongful act to comply with its international obligations as reflected in the Articles on State Responsibility adopted by the International Law Commission (ILC) in 2001 (Articles 22 and 49–54).[4] Application of this instrument presupposes that the conduct to be countered is attributable to a State.[5] As far as a cyber operation by a non-State actor cannot be attributed, countermeasures against a State will be available only to the extent that there has been a related breach of a due diligence obligation by that particular State.[6] Moreover, the law of countermeasures does not justify an encroachment upon the rights of a third State not responsible for an internationally wrongful act.[7] But active cyber defenses often do have unintended effects on third States due to the high level of interconnectedness and interdependency of digital infrastructure. This is the case, for example, where a State reacts to a malicious cyber operation with shutting down foreign infrastructure that has a key function for communication in a larger region. The fact that a certain response is lawful as a countermeasure vis-à-vis one particular State does not make it lawful per se. In relation to other States, the measure may still constitute a breach of an international obligation.[8] Here the plea of necessity could come into play as a circumstance precluding wrongfulness. In constellations in which neither the right to self-defense nor the law of countermeasures applies, "the plea of necessity may present the sole option for a response that would otherwise be unlawful."[9] Unlike self-defense and countermeasures, necessity does not

---

that would limit the right to self-defense to armed attacks by States); *see also* TALLINN MANUAL 2.0, *supra* note 1, at 345 (recognizing that the issue of whether acts of non-State actors can constitute an armed attack absent involvement by a State is controversial); Daniel Bethlehem, *Self-Defense Against an Imminent or Actual Armed Attack by Nonstate Actors*, 106 AM. J. INT'L L. 770, 774 (2012) (noting "[i]t is by now reasonably clear and accepted that states have a right of self-defense against attacks by nonstate actors").

4. Draft Articles on Responsibility of States for Internationally Wrongful Acts, Int'l Law Comm'n, Rep. on the Work of Its Fifty-Third Session, U.N. G.A.O.R., 56th Sess., U.N. Doc. A/56/10 (Supplement No. 10), at 43 (2001), *reprinted in* [2001] 2 Y.B. Int'l L. Comm'n 26, U.N. Doc. A/CN.4/SER.A/2001/Add.1 (Part 2) [hereinafter ARSIWA]; *see also* G.A. Res. 56/83, annex (Dec. 12, 2001) (setting forth the Articles).

5. ARSIWA, *supra* note 4, art. 49, para. 4.

6. TALLINN MANUAL 2.0, *supra* note 1, at 113.

7. ARSIWA, *supra* note 4, art. 49, para. 4 (stating that an injured State may only take countermeasures against the responsible State).

8. TALLINN MANUAL 2.0, *supra* note 1, at 133 (Rule 25).

9. *Id.* at 138; *see also* Michael N. Schmitt & M. Christopher Pitts, *Cyber Countermeasures and Effects on Third Parties: The International Legal Regime*, 14 BALTIC Y.B. INT'L L. 1, 14–15 (2014) (noting that "the plea of necessity allows for a broader range of effects on third States than is permissible with countermeasures").

depend on prior unlawful conduct and does not require attribution.[10] A state of necessity may just as well be brought about by a natural disaster. Robin Geiß and Henning Lahmann described the character of the plea of necessity as follows: "the question is not who or what caused the situation, but only what is necessary in order to avert the danger or mitigate the harm caused by the situation."[11]

Traditionally, necessity has been understood as a subjective right of the State to self-preservation. In this sense, the roots of the doctrine can be traced back to the sixteenth and seventeenth century, in particular to the writings of Alberico Gentili and Hugo Grotius, as well as to the eighteenth century works of Emer de Vattel on the law of nations.[12] But the modern concept of necessity has been completely detached from these roots. It is not limited anymore to safeguarding the survival of the State.[13] Sarah Heathcote characterizes necessity in contemporary international law as nothing more than an exception that, "far from being a subjective right, simply permits, under certain circumstances, the temporary non-execution of an international obligation" for the purpose of managing an unforeseen crisis.[14] A fundamental question, which will not be discussed in this essay, is whether the plea of necessity may also cover the use of force. While *Tallinn Manual 2.0* leaves this question unanswered,[15] the present author is of the opinion that necessity does not provide a separate legal basis for military action. The prohibition on the use of force laid down in Article 2 (4) of the U.N. Charter has the character of *jus cogens*; and as a circumstance precluding wrongfulness, the plea of necessity does not justify or excuse any derogation from a peremptory norm of general international law.[16] Possible exceptions

---

10. *See* ARSIWA, *supra* note 4, art. 25, para. 2 (explaining that the plea of necessity "is not dependent on the prior conduct of the injured State").

11. 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 621, 644 (Katharina Ziolkowski ed., 2013).

12. *See, e.g.*, Roberto Ago (Special Rapporteur), *Addendum to the Eighth Rep. on State Responsibility*, U.N. Doc. A/CN.4/318/Add.5-7, at 46 (1980), *reprinted in* [1980] 2 Y.B. Int'l L. Comm'n 13, U.N. Doc. A/CN.4/SER.A/1980/Add.1 (Part 1) (identifying Alberico Gentili and Hugo Grotius as "classical writers" in the field of international law during the sixteenth and seventeenth centuries, and Emer de Vattel during the eighteenth century, who considered necessity to be a natural right of States); Roman Boed, *State of Necessity as a Justification for Internationally Wrongful Conduct*, 3 YALE HUM. RTS. & DEV. L.J. 1, 4–7 (2000) (discussing Hugo Grotius's early writings on necessity as a right to self-preservation).

13. Ago, *supra* note 12, at 17.

14. Sarah Heathcote, *Circumstances Precluding Wrongfulness in the ILC Articles on State Responsibility: Necessity*, *in* THE LAW OF INTERNATIONAL RESPONSIBILITY 491, 492 (James Crawford, Alain Pellet & Simon Olleson eds., 2010).

15. TALLINN MANUAL 2.0, *supra* note 1, at 140.

16. ARSIWA, *supra* note 4, art. 26; *see also* Olivier Corten, *Necessity*, *in* THE OXFORD HANDBOOK OF THE USE OF FORCE IN INTERNATIONAL LAW 861, 863–67 (Marc Weller ed., 2015) (examining the inability to claim necessity to justify military force in violation of the U.N. Charter).

to the prohibition on the use of force may only be construed on the basis of a primary norm of international law such as the right to self-defense or the authority of the Security Council to take binding decisions under Chapter VII of the U.N. Charter.[17]

Nevertheless, it is important to stress that the plea of necessity generally involves a high risk of abuse because it may be invoked to justify measures that violate the rights of other States irrespective of whether these States are in any way responsible for the situation.[18] James Crawford once noted that necessity stood at the "outer edge of the tolerance of international law for otherwise wrongful conduct."[19] Therefore it is widely accepted that the plea of necessity is available only in exceptional cases and subject to strict limitations. The ILC commentary on Article 25 of the Articles on State Responsibility, which defines necessity as one of six circumstances precluding wrongfulness, cautions that necessity "will only rarely be available."[20] The plea's general susceptibility to abuse gives particular cause for concern in the cyber context. A dramatic increase in malicious cyber activity, the speed at which cyber incidents can occur, and the difficulty of identifying the sources of such incidents have already heightened the risk of escalation of inter-State conflict within and beyond cyberspace. Where States may be inclined to invoke necessity as a pretext for interfering with foreign cyber infrastructure, the potential for escalation is extremely high and the consequences are incalculable. Under such conditions an excessive invocation of the plea of necessity might, in the longer term, even have a destabilizing effect on international peace and security. Against this background, Rule 26 of *Tallinn Manual 2.0* needs to be critically assessed.

First, the basic parameters of the concept of necessity as understood in Rule 26 are briefly described in Part I. In Part II, it will be examined to what extent this understanding actually reflects customary international law. Then the focus will be on interpretation of Rule 26. While each element of this Rule deserves closer attention, Part III of the present essay concentrates on several threshold criteria that are particularly open to wide interpretation, which could abet excessive invocation and possible abuses of the plea of necessity in the cyber context. Taking into regard the heightened risk of escalation, it will finally be argued in Part IV that States should develop a more specific multilateral framework with particular emphasis on procedural

17. ARSIWA, *supra* note 4, art. 25, para. 21.

18. *See, e.g.*, JAMES CRAWFORD, STATE RESPONSIBILITY: THE GENERAL PART 305–06 (2013) (describing abuses of necessity by Germany in the First and Second World Wars as well as previous abuses by other States); Heathcote, *supra* note 14, at 492 (noting the abuses that have resulted from claims of necessity).

19. Int'l Law Comm'n, Rep. on the Work of Its Fifty-First Session, U.N. G.A.O.R., 54th Sess., U.N. Doc. A/54/10 (Supplement No. 10), at 184 (1999), *reprinted in* [1999] 2 Y.B. Int'l L. Comm'n 1, U.N. Doc. A/CN.4/SER.A/1999/Add.1 (Part 2).

20. ARSIWA, *supra* note 4, art. 25, para. 2.

standards for resolving cyber incidents that rise to the level of a state of necessity.

I. The Conception of Necessity Embodied in Rule 26 of *Tallinn Manual 2.0*

In the 2013 *Tallinn Manual on the International Law Applicable to Cyber Warfare*, which was the predecessor version of *Tallinn Manual 2.0*, necessity was only briefly addressed in the context of countermeasures in order to illustrate the differences between the two concepts.[21] *Tallinn Manual 2.0* deals with the plea of necessity in a more detailed way. Rule 26 provides: "A State may act pursuant to the plea of necessity in response to acts that present a grave and imminent peril, whether cyber in nature or not, to an essential interest when doing so is the sole means of safeguarding it."[22]

Rule 26 consists of three elements: There must be a "grave and imminent peril" to an "essential interest" and the action taken must be the "sole means" of safeguarding that interest. The sole-means requirement mirrors the very nature of the plea of necessity. As long as there are other means available, even if they are more costly or less convenient, the act in question is "not *necessary* in the strict sense of the term."[23]

Rule 26 is based on Article 25 of the ILC Articles on State Responsibility.[24] Article 25, which has a more complex structure, accentuates the exceptional character of the plea of necessity by its negative wording ("Necessity may not be invoked . . . unless . . . ."),[25] whereas Rule 26 of *Tallinn Manual 2.0* is formulated as a positive authorization ("A State may act pursuant to the plea of necessity . . . when . . . .").[26] As far as the conditions for action are concerned, Article 25 of the ILC Articles on State Responsibility contains two additional requirements. First, the act must

---

21. TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE 39–40 (Michael N. Schmitt ed., 2013).

22. TALLINN MANUAL 2.0, *supra* note 1, at 135 (Rule 26).

23. Geiß & Lahmann, *supra* note 11, at 649.

24. Article 25 of ARSIWA provides:

> 1. Necessity may not be invoked by a State as a ground for precluding the wrongfulness of an act not in conformity with an international obligation of that State unless the act:
> (a) is the only way for the State to safeguard an essential interest against a grave and imminent peril; and
> (b) does not seriously impair an essential interest of the State or States towards which the obligation exists, or of the international community as a whole.
> 2. In any case, necessity may not be invoked by a State as a ground for precluding wrongfulness if:
> (a) the international obligation in question excludes the possibility of invoking necessity; or
> (b) the State has contributed to the situation of necessity.

ARSIWA, *supra* note 4, art. 25.

25. *Id.*

26. TALLINN MANUAL 2.0, *supra* note 1, at 135 (Rule 26).

"not seriously impair an essential interest of the State or States towards which the obligation exists, or of the international community as a whole."[27] The ILC commentary on Article 25 states that "the interest relied on must outweigh all other considerations, not merely from the point of view of the acting State but on a reasonable assessment of the competing interests, whether these are individual or collective."[28] Second, according to Article 25, necessity may not be invoked by a State that has contributed to the situation. For the plea to be precluded, the contribution must be "sufficiently substantial and not merely incidental or peripheral."[29] One may speculate why these two additional conditions have not been included in the text of Rule 26 of *Tallinn Manual 2.0*. It is important to emphasize, however, that the commentary on Rule 26 considers both requirements to be integral components of this Rule.[30] This means that the conception of necessity embodied in *Tallinn Manual 2.0* is in fact subject to more stringent requirements than the plain wording of Rule 26 may suggest. Despite some textual differences, there is thus no substantial discrepancy between Rule 26 of *Tallinn Manual 2.0* and Article 25 of the ILC Articles on State Responsibility.

II. Rule 26 and Customary International Law

Tallinn Manual 2.0 is "intended as an objective restatement of the *lex lata*" and its authors claimed that they "assiduously avoided including statements reflecting *lex ferenda*."[31] There is no doubt that the plea of necessity as such is rooted in customary international law. More questionable is whether the specific understanding of necessity promoted by the commentary on Rule 26 is really an objective restatement of the *lex lata*. To the knowledge of the present author, there is not yet any State practice that could demonstrate how necessity is invoked in response to cyber incidents. Therefore, one has to rely on the "classic" necessity cases when exploring to what extent the *Tallinn Manual 2.0*'s notion of necessity reflects customary international law. For this purpose it is instructive to take a closer look at the cases referred to by the ILC in the 2001 commentary on Article 25 of the Articles on State Responsibility.[32] These cases can be roughly grouped into

27. ARSIWA, *supra* note 4, art. 25.

28. *Id.* art. 25, para. 17.

29. *Id.* art. 25, para. 20.

30. TALLINN MANUAL 2.0, *supra* note 1, at 137, 140–41. According to the commentary, it is a "key limitation" that a State invoking the plea of necessity may not engage in cyber operations that seriously impair the essential interests of affected States. *Id.* at 137. In terms of contribution, it is clarified, inter alia, that the mere failure of a State to adequately protect its own cyber infrastructure against harmful cyber operations did not bar the State from taking measures based on necessity. *Id.* at 140.

31. *Id.* at 3.

32. The commentary concentrates on nine cases in which the plea of necessity "has been accepted in principle, or at least not rejected." ARSIWA, *supra* note 4, art. 25, paras. 3–12.

three categories: security-related necessity, economic necessity, and environmental necessity.[33]

In the Anglo-Portuguese dispute of 1832, which illustrates an early concept of security-related necessity, the Portuguese Government appropriated property owned by British subjects in order to subsist troops that were engaged in quelling internal disturbances.[34] In this case, the British Government was advised by its law officers that a treaty which had been concluded between both countries to protect the property of British nationals residing in Portugal did not deprive the Portuguese Government of the right of using those means "which may be absolutely and indispensably necessary to the safety, and even to the very existence of the State."[35] In the *Caroline* case of 1837, which falls into the same category, the British Government justified a raid on U.S. territory with the "necessity of self-defence and self-preservation."[36] U.S. Secretary of State Daniel Webster replied that "nothing less than a clear and absolute necessity can afford ground of justification."[37] Lord Ashburton, the British Government's ad hoc envoy, later spoke of "a strong overpowering necessity" that could—"for the shortest possible period" and "within the narrowest limits"—suspend the obligation to respect the independent territory of another State.[38] While both cases may be regarded as early precedents backing the existence of the plea of necessity as such, it is important to note that none of the parties felt compelled to weigh the competing interests.[39]

The second category of cases relates to economic crises. In the *Russian Indemnity* case,[40] a controversy between Russia and Turkey regarding a claim for interest on deferred payment of indemnities to Russian subjects for losses incurred during the Russo–Turkish War of 1877–1878, the Russian

---

33. *See* Robert D. Sloane, *On the Use and Abuse of Necessity in the Law of State Responsibility*, 106 AM. J. INT'L L. 447, 454 (2012) (stating that the categories of cases and incidents quoted in the ILC commentary correspond to three different paradigms: "classical necessity," "economic necessity," and "ecological necessity").

34. *See* Int'l Law Comm'n, Rep. on the Work of Its Thirty-Second Session, U.N. G.A.O.R., 35th Sess., U.N. Doc. A/35/10 (Supplement No. 10), at 84 (1980), *reprinted in* [1980] 2 Y.B. Int'l L. Comm'n 1, U.N. Doc. A/CN.4/SER.A/1980/Add.1 (Part 2) (discussing the Anglo-Portuguese dispute).

35. *Id.*

36. ARSIWA, *supra* note 4, art. 25, para. 5; *see The Caroline*, *in* MAX PLANCK ENCYCLOPEDIA OF PUBLIC INTERNATIONAL LAW (Online ed. 2016), http://opil.ouplaw.com/home/epil [https://perma.cc/8VZD-LRAU] [hereinafter MPIL] (summarizing the facts of the *Caroline* case and its impact on public international law).

37. 29 BRITISH AND FOREIGN STATE PAPERS 1840–1841 1133, 1137–38 (1857).

38. 30 BRITISH AND FOREIGN STATE PAPERS 1841–1842 196 (1858).

39. *See* Sloane, *supra* note 33, at 457–58 (commenting that the parties in the *Caroline* case effectively "agree[d] to disagree" about whether Britain's conduct conformed to the legal principles of necessity).

40. Affaire de l'indemnité russe (Russie v. Turquie), 11 R.I.A.A. 421 (Perm. Ct. Arb. 1912), *translated in Judicial Decisions Involving Questions of International Law: Russia versus Turkey*, 7 AM. J. INT'L L. 178 (1913).

Government acknowledged that the obligation of a State to fulfill a treaty may give way if the very existence of the State was in danger and if the observance of the international duty was self-destructive.[41] Like the Anglo-Portuguese dispute and the *Caroline* incident, this case reflects the traditional conception of necessity that presupposes an existential threat to the State concerned.[42] Another case in the category of economic necessity, *Société Commerciale de Belgique*,[43] was decided by the Permanent Court of International Justice in 1939. This reference might be considered as offering some support for the transition from "the classical, existential threshold for necessity" to "the lower threshold and broader scope" of the notion of "essential interest."[44] The parties, Greece and Belgium, concurred and the court seemed to have accepted that a debtor State would not incur responsibility if paying the debt would jeopardize the country's economic existence and the normal operation of essential public services or disturb public order and social tranquility.[45] But—like in the above-mentioned cases—the "idea of comparing or balancing the essential interests" of the parties did not play any role in the pleadings or the judgment.[46]

Other cases cited by the ILC may be subsumed under the category of environmental necessity. The reference to both the *Russian Fur Seals* controversy of 1893[47] and the *Fisheries Jurisdiction* case decided by the International Court of Justice (ICJ) in 1998[48] has been described by Robert Sloane as "not especially helpful" and "inapposite" to support Article 25 of the ILC Articles on State Responsibility because no evidence suggested that the parties actually regarded these incidents as involving the plea of necessity as a legal defense.[49] The background of the *Russian Fur Seals* controversy was that Russia, in an attempt to avert the danger of extermination of a fur-seal population on the high seas near its territorial waters, seized several British sealing vessels and issued a decree that prohibited the hunting of seals

41. *Id.* at 443; *see also* Sloane, *supra* note 33, at 461 (analyzing the *Russian Indemnity* case and Russia's admission that treaty obligations give way to circumstances that threaten the existence of the State).

42. Sloane, *supra* note 33, at 461.

43. Société Commerciale de Belgique (Belg. v. Greece), Judgment, 1939 P.C.I.J. (ser. A/B) No. 78, at 160 (June 15).

44. Sloane, *supra* note 33, at 464.

45. *See* Int'l Law Comm'n, *supra* note 34, at 76–79 (reporting that Belgian counsel agreed with the principle that "a State is not obliged to pay its debt if in order to pay it it would have to jeopardize its essential public services" and positing that the court "implicitly accepted" this principle); Belg. v. Greece, 1939 P.C.I.J. at 177–78 (explaining that if the court were to rule on Greece's actions, which the court would not presently do, it could only do so "after having itself verified that the alleged financial situation really exists and after having ascertained the effect which the execution of the awards in full would have on that situation").

46. Sloane, *supra* note 33, at 466.

47. ARSIWA, *supra* note 4, art. 25, para. 6.

48. Fisheries Jurisdiction (Spain v. Can.), Judgment, 1998 I.C.J. 432 (Dec. 4).

49. Sloane, *supra* note 33, at 467–68.

in this particular area.[50] In a letter to the British Ambassador, the Russian Minister for Foreign Affairs stressed the "absolute necessity of immediate provisional measures" in view of the imminence of the hunting season and emphasized that the measures were taken "under the pressure of exceptional circumstances."[51] A similar line of argument was brought forward by Canada a hundred years later in the *Fisheries Jurisdiction* case, which concerned the seizure of a Spanish fishing vessel by Canadian officials 245 miles off the Canadian coast.[52] The Canadian government claimed that the arrest of the vessel, based on the Canadian Coastal Fisheries Protection Act, "was necessary in order to put a stop to the overfishing of Greenland halibut by Spanish fishermen."[53] But Canada did not even consider itself under pressure to justify a wrongful act.[54] Even if both cases are regarded as backing the existence of the necessity doctrine in international law, Sloane rightly observed that it was difficult to see how these cases should support the particular conception of necessity set forth in Article 25 of the ILC Articles on State Responsibility. Neither Russia nor Canada argued that the essential interests at stake outweighed all other considerations.[55]

A case that is often cited as a precedent for the plea of necessity in the context of ecological disasters is the *Torrey Canyon* incident of 1967.[56] The *Torrey Canyon* was a Liberian oil tanker, which went aground in international waters off the coast of Cornwall.[57] After various failed attempts to contain the oil spill, the United Kingdom bombed the vessel to burn the oil remaining on board.[58] The operation, which was successful, did not evoke any protests either from the owner of the ship or from other governments, and the British Government did not submit any legal justification for its conduct.[59] Instead, it simply stressed the existence of a situation of extreme danger and asserted that the decision to bomb the ship had been taken only after all other means had failed.[60]

The ICJ made a prominent statement on the plea of necessity in the 1997 *Gabčíkovo-Nagymaros Project* judgment.[61] The background of this case was

50. *See* Int'l Law Comm'n, *supra* note 34, at 81–82.

51. *Id.* at 81 (quoting from the letter of the Russian Minister for Foreign Affairs to the British Ambassador).

52. Spain v. Can., 1998 I.C.J. at 443, para. 20.

53. *Id.*

54. Sloane, *supra* note 33, at 469.

55. *Id.*

56. *See The Torrey Canyon*, *in* MPIL, *supra* note 36 (noting the *Torrey Canyon*'s significance in the development of the doctrine of necessity, especially in the ecological context).

57. *Id.*

58. *Id.*

59. *Id.*

60. *Id.*

61. Gabčíkovo-Nagymaros Project (Hung. v. Slovk.), Judgment, 1997 I.C.J. 7, 35–46 (Sept. 25).

a dispute between Hungary and Slovakia over the construction of dam structures on the river Danube.[62] In 1977, Hungary and Czechoslovakia had concluded a treaty for the building of such structures.[63] In 1989, Hungary stopped completion of the project, alleging that it entailed grave risks to its environment.[64] The ICJ considered the question of "whether there was, in 1989, a state of necessity which would have permitted Hungary, without incurring international responsibility, to suspend and abandon works that it was committed to perform [under] the 1977 Treaty."[65] Inter alia, the ICJ acknowledged that the state of necessity was recognized by customary international law as a ground for precluding wrongfulness in exceptional cases.[66] Since the parties were in agreement that the existence of a state of necessity had to be evaluated in light of the criteria laid down in Article 33 of the Draft Articles on State Responsibility[67] (which, as revised, became Article 25 of the Articles on State Responsibility),[68] the ICJ examined these conditions and found that they had not been met.[69] It is noteworthy, however, that the ICJ did not refer to any State practice and *opinio juris* to substantiate its assertion concerning the customary nature of the plea of necessity.[70]

Other authorities that confirm the customary character of the plea of necessity include the judgment of the International Tribunal for the Law of the Sea (ITLOS) of 1999 in the *M/V "Saiga" (No. 2)* case[71] and the advisory opinion of the ICJ of 2004 on *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*.[72] In the *M/V "Saiga" (No. 2)* case, ITLOS referred to the *Gabčíkovo-Nagymaros Project* judgment and insinuated that the ICJ had pronounced that the specific conditions mentioned in Draft Article 33 reflected customary international law.[73] Yet it is by no means clear whether the ICJ had actually intended to go that far. The ICJ could have easily stated that Draft Article 33 per se was an expression of international custom, but it did not do so. Even seven years later, in the *Legal*

62. Gabčíkovo-Nagymaros Case (Hungary/Slovakia), *in* MPIL, *supra* note 36.

63. *See* Hung. v. Slovk., 1997 I.C.J. at 17–24, paras. 15–20 (quoting the relevant provisions of the Treaty).

64. *Id.* at 25, para. 22, 35–36, para 40.

65. *Id.* at 39, para. 49.

66. *Id.* at 40, para. 51.

67. *Id.* at 39–40, para. 50.

68. *See* Draft Articles on State Responsibility, Int'l Law Comm'n, Rep. on the Work of Its Thirty-Second Session, U.N. G.A.O.R., 35th Sess., U.N. Doc. A/35/10 (Supplement No. 10), at 59, 68 (1980), *reprinted in* [1980] 2 Y.B. Int'l L. Comm'n 30, U.N. Doc. A/CN.4/SER.A/1980/Add.1 (Part 2) (setting forth the language of Article 33 of the Draft Articles on State Responsibility).

69. *Id.* at 40–46, paras. 52–59.

70. *See id.*

71. M/V Saiga (No. 2) (St. Vincent v. Guinea), Case No. 2, Judgment of July 1, 1999, https://www.itlos.org/cases/list-of-cases/case-no-2/#c2091 [https://perma.cc/NPV7-FEAL].

72. Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion, 2004 I.C.J. 136 (July 9) [hereinafter Legal Consequences].

73. Saint Vincent v. Guinea, at paras. 133–34.

Consequences advisory opinion of 2004, the ICJ recognizably shied away from such an all-out endorsement.[74]

A number of arbitral decisions concerning Argentina's fiscal crisis around 2000–2001 also dealt with necessity under customary international law.[75] In considering whether the crisis had met the requirements of Article 25 of the ILC Articles on State Responsibility, the tribunals and ad hoc committees in most cases elaborated on whether Argentina's breaches of financial obligations seriously impaired essential interests of the States towards which the obligations existed, and whether Argentina had substantially contributed to the crisis.[76] These tribunals and committees routinely presumed that Article 25 adequately reflected the state of customary international law.[77] For them it was simply comfortable to rely on Article 25 in order to have some standard for tackling the questions at hand. But it seems that they did not spend any effort to show why they considered Article 25 to reflect customary international law (with the exception of the International Arbitral Tribunal in *CMS Gas Transmission Co. v. Argentine Republic*, which at least pointed to some of the above-mentioned cases contained in the ILC commentary on Article 25).[78]

To sum up, all these cases may be regarded as providing a sound basis for arguing in favor of the customary legal nature of the plea of necessity as such; and the plain text of Rule 26 of *Tallinn Manual 2.0* with its three elements ("essential interest," "grave and imminent peril," "sole means")

---

74. Legal Consequences, *supra* note 72, at 194–95, para. 140 (clarifying only that the ICJ in the *Gabčíkovo-Nagymaros Project* judgment had referred to "a text" by the International Law Commission (Article 33 of the Draft Articles), "which in its current form" (Article 25) required, inter alia, that the act in question had to be the only way for the State to safeguard an essential interest against a grave and imminent peril).

75. *E.g.*, CMS Gas Transmission Co. v. Arg. Republic, ICSID Case No. ARB/01/8, Award, paras. 315–31 (May 12, 2005); LG&E Energy Corp. v. Arg. Republic, ICSID Case No. ARB/02/1, Decision on Liability, paras. 245–57 (Oct. 3, 2006); Enron Corp. v. Arg. Republic, ICSID Case No. ARB/01/3, Award, paras. 294–313 (May 22, 2007); Sempra Energy Int'l v. Arg. Republic, ICSID Case No. ARB/02/16, Award, paras. 333–54 (Sept. 28, 2007). For further references, see U.N. Secretary-General, *Responsibility of States for Internationally Wrongful Acts—Compilation of Decisions of International Courts, Tribunals and Other Bodies*, U.N. Doc. A/62/62, paras. 95–96 (Feb. 1, 2007); U.N. Doc. A/65/76, para. 26 (Apr. 30, 2010); U.N. Doc. A/68/72, paras. 90–98 (Apr. 30, 2013); U.N. Doc. A/71/80, paras. 93–94 (Apr. 21, 2016); *see also* Marie Christine Hoelck Thjoernelund, *State of Necessity as an Exemption from State Responsibility for Investments*, 13 MAX PLANCK Y.B. U.N. L. 423 (2009) (discussing necessity as an exemption from State responsibility in the context of the above Argentine fiscal crisis cases).

76. *E.g.*, CMS Gas Transmission Co. v. Arg. Republic, ICSID Case No. ARB/01/8, paras. 325, 328–29, 357–58; LG&E Energy Corp. v. Arg. Republic, ICSID Case No. ARB/02/1, paras. 254, 256–57; Enron Corp. v. Arg. Republic, ICSID Case No. ARB/01/3, paras. 310–12, 341–42; Sempra Energy Int'l v. Arg. Republic, ICSID Case No. ARB/02/16, paras. 352–54, 390–91.

77. *E.g.*, CMS Gas Transmission Co. v. Arg. Republic, ICSID Case No. ARB/01/8, para. 315; LG&E Energy Corp. v. Arg. Republic, ICSID Case No. ARB/02/1, para. 245; Enron Corp. v. Arg. Republic, ICSID Case No. ARB/01/3, para. 303; Sempra Energy Int'l v. Arg. Republic, ICSID Case No. ARB/02/16, para. 344.

78. CMS Gas Transmission Co. v. Arg. Republic, ICSID Case No. ARB/01/8, para. 315.

seems to be an adequate reflection of customary international law. But some doubts remain with regard to the requirement that the action must not seriously impair the essential interests of other States. Many writers have assumed without further examination that this element was an integral part of the concept of necessity. Most of them have simply referred to Article 25 of the ILC Articles on State Responsibility.[79] In State practice, however, it is difficult to find sufficient evidence for upholding this assumption. It is somewhat telling that the Arbitral Tribunal in the *Rainbow Warrior* arbitration of 1990,[80] which is also mentioned as a source of authority in the ILC commentary on Article 25,[81] has emphasized the "controversial character" of the proposal made in Draft Article 33 (which later became Article 25).[82] Robert Sloane, who has conducted an in-depth analysis on the matter, shows that the balancing-of-interests requirement actually has its origin in national criminal law systems. Moreover, he offers good arguments for being very skeptical about transferring this element to the sphere of necessity in international law by way of a simple national-law analogy.[83] In any case, the fact that there remains some uncertainty in this regard at least makes it easier for States to act in the name of necessity without properly assessing and balancing the consequences of their action in relation to the essential interests of other States. But with the evolution of cyber-related State practice, the contours of the plea of necessity as applied to cyber incidents may become clearer.

III. Interpreting the Thresholds of Rule 26

This section focuses on the threshold criteria contained in Rule 26 of *Tallinn Manual 2.0*. First, it is important to recall that a state of necessity arises only if an *essential* interest of a State is endangered.[84] Therefore it needs to be clarified which interests of a State are sufficiently essential to be covered by Rule 26. Second, necessity presupposes that an essential interest is endangered by a *grave and imminent* peril.[85] Essentiality, gravity, and imminence are thus key qualifiers for identifying situations of a certain pressing quality that rise to the level of necessity. An evaluation of whether the action taken is in conformity with the other requirements outlined in

79. *See, e.g.*, Geiß & Lahmann, *supra* note 11, at 649–50 (offering some discussion of what serious impairment of States' essential interests as an element of Article 25 may involve); Heathcote, *supra* note 14, at 498; Avidan K. Kent & Alexandra R. Harrington, *A State of Necessity: International Obligations in Times of Crises*, 42 CAN. REV. AM. STUD. 65, 67 (2012) (accepting Article 25 as the statement of the necessity doctrine); Thjoernelund, *supra* note 75, at 438 (looking to Article 25 as source for elements of necessity).

80. Rainbow Warrior (N.Z. v. Fr.), 20 R.I.A.A. 215 (Arb. Trib. 1990).

81. ARSIWA, *supra* note 4, art. 25, para. 10.

82. N.Z. v. Fr., 20 R.I.A.A. at 254.

83. Sloane, *supra* note 33, at 458–59, 478–81.

84. TALLINN MANUAL 2.0, *supra* note 1, at 135 (Rule 26).

85. *Id.*

Rule 26 and the accompanying commentary, i.e., whether the action is the sole means and does not seriously impair the essential interests of other States, may also be highly problematic from case to case. But an interpretation of these conditions is beyond the scope of the present essay.

A. Essentiality of the Endangered Interest

The *Tallinn Manual*'s commentary on Rule 26 circumscribes essentiality as "of fundamental and great importance to the State concerned."[86] At the same time, it points to the vagueness of this term and asserts that essentiality of a particular interest "is always contextual" and may "vary from State to State."[87] In particular, the commentary notes the tendency of States designating certain infrastructure as "critical."[88] Based on this observation, it may be argued that the integrity of critical infrastructure qualifies as an essential interest within the meaning of Rule 26.[89] According to the commentary, however, a State's unilateral classification of infrastructure as "critical" could not be determinative of the issue.[90] If the decision was solely within the domain of each State, the plea of necessity would probably lose its exceptional character. States could be inclined to invoke necessity as a pretext for evading inconvenient obligations in various fields by simply claiming that the interests at stake are essential. Sarah Heathcote therefore held that there needed to be a certain social consensus amongst the international community that a particular interest was indeed essential.[91]

In this regard it deserves to be mentioned that Australia, Canada, New Zealand, the United Kingdom, and the United States in 2014 proposed a common definition of "critical infrastructure."[92] The definition encompasses "the systems, assets, facilities and networks that provide essential services and are necessary for the national security, economic security, prosperity, and health and safety of their respective nations."[93] Moreover, the five countries identified certain sectors that all of them consider to be critical: communications, energy, healthcare and public health, transportation systems, and water.[94] In addition, several members of the group also

86. *Id.* at 135.

87. *Id.*; *see also* ARSIWA, *supra* note 4, art. 25, para. 15 ("The extent to which a given interest is 'essential' depends on all the circumstances, and cannot be prejudged.").

88. TALLINN MANUAL 2.0, *supra* note 1, at 135.

89. *See, e.g.*, Geiß & Lahmann, *supra* note 11, at 646 ("[I]t seems reasonable to assume that at least the protection of critical infrastructure would be accepted as such an essential interest . . . .").

90. TALLINN MANUAL 2.0, *supra* note 1, at 135–36.

91. Heathcote, *supra* note 14, at 497.

92. *Forging a Common Understanding for Critical Infrastructure—Shared Narrative*, CRITICAL 5 (Mar. 2014), https://www.dhs.gov/sites/default/files/publications/critical-five-shared-narrative-critical-infrastructure-2014-508.pdf [https://perma.cc/HWU3-342S].

93. *Id.*

94. *Id.* at 6.

highlighted the following sectors as critical: banking and financial services, critical manufacturing, emergency services, food and agriculture, government facilities, and information technology.[95] The criticality criterion may also be accentuated by pointing to the serious consequences that the disablement or destruction of such infrastructure would have. One should be aware, though, that China, Russia, and other States that follow a particular understanding of "information security"[96] will also have different preferences regarding the scope of the concept of critical infrastructure.

An interesting question is whether election infrastructure (voter-registration systems, voting machines, tabulation systems, etc.) may be classified as critical.[97] Foreign interference with elections is a phenomenon that has gained new attention during the 2016 presidential election campaign in the United States.[98] Germany and other European countries are also well aware that their upcoming elections could be targeted by hackers. The German intelligence agencies, for instance, have already indicated that they would be willing to resort to counter-hacking and active cyber defenses to the extent that national security law provided them with sufficient authority to do so.[99]

Apart from that, the debate over what could constitute an essential interest within the meaning of Rule 26 should not be narrowed down solely to the concept of critical infrastructure. Other interests that might be considered essential could relate to the territorial integrity, political independence, and constitutional order of the State, the maintenance of public security, and the preservation of the natural environment of the State.

B. Gravity and Imminence of the Peril

"Peril" can be defined as a situation in which harm is likely to occur if no preventive action is taken. Of the two threshold criteria qualifying peril within the meaning of Rule 26 of *Tallinn Manual 2.0*, "gravity" seems to be

---

95. *Id.*

96. *See* U.N. Secretary-General, Letter dated Jan. 9, 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan, and Uzbekistan to the United Nations, U.N. Doc. A/69/723 (Jan. 13, 2015) (submitting "an international code of conduct for information security" to the General Assembly).

97. *See* Scott J. Shackelford et al., *Making Democracy Harder to Hack: Should Elections Be Classified as 'Critical Infrastructure?'*, 50 MICH. J.L. REFORM 629 (forthcoming 2017) (identifying a wide range of technical vulnerabilities in the election process).

98. *See, e.g.*, Jens David Ohlin, *Did Russian Cyber Interference in the 2016 Election Violate International Law?*, 95 TEXAS L. REV. 1579, 1580 (2017) (assessing Russian interference in the election using a "self-determination" framework rather than a "sovereignty" framework).

99. *Verfassungsschutz will Cybergegenangriffe starten*, SPIEGEL ONLINE (Jan. 10, 2017), http://www.spiegel.de/netzwelt/netzpolitik/bundesamt-fuer-verfassungsschutz-plant-cyber-gegenangriffe-a-1129273.html [https://perma.cc/W6PA-RSDR]; *see also* Andrea Shalal, *Europe Erects Defenses to Counter Russia's Information War*, REUTERS (Jan. 12, 2017), http://www.reuters.com/article/us-usa-cyber-russia-europe-idUSKBN14W2BY [https://perma.cc/VPD3-C2AR] (reporting on European responses to Russian cyber interference).

less controversial (although it is just as vague as the term "essential"). "Gravity" relates to the scale and effects of the expected harm. A peril may be assumed to be grave if it interferes with an interest "in a fundamental way, like destroying the interest or rendering it largely dysfunctional."[100] "Mere inconvenience, irritation, or minor disruption" does not suffice.[101] The gravity element will usually be fulfilled if a cyber operation is of such quality that it could disable or destroy critical infrastructure.[102]

The notion of imminence is more problematic. It has already gained considerable attention in the debate on the right to anticipatory self-defense.[103] Imminence generally requires that the expected harm is identifiable, specific, and is likely to occur in the immediate future.[104] In the ILC commentary on Article 25 of the Articles on State Responsibility, it is expounded that the peril had to be "imminent in the sense of proximate."[105] But the *Gabčíkovo-Nagymaros Project* judgment of the ICJ contains a remarkable statement that relativizes the requirement of temporal proximity. In the view of the ICJ, a peril appearing in the long term might be classified as imminent "as soon as it is established, at the relevant point in time, that the realization of that peril, however far off it might be, is not thereby any less certain and inevitable."[106] This means that an imminent peril may even exist where the harm will probably occur in a more remote future. A typical case of a peril materializing over time is a cyber operation targeting the banking system or stock market. While such an operation has certain immediate effects, it is the long-term impact, in particular the loss of confidence in the system and the ensuing shock waves in the financial sector, that would qualify the incident as a "grave and imminent peril."[107] The ICJ approach thus suggests that there is a relatively broad spectrum of cases in which a peril may be considered imminent. On the one end of the spectrum are situations in which it is sufficiently certain that the harm is just about to occur, whereas on the other end there are situations in which it is not "any

100. TALLINN MANUAL 2.0, *supra* note 1, at 136.

101. *Id.*

102. *Id.* at 136–37.

103. *See, e.g.*, Dapo Akande & Thomas Liefländer, *Clarifying Necessity, Imminence, and Proportionality in the Law of Self-Defense*, 107 AM. J. INT'L L. 563, 564–66 (2013) (attempting to clarify the concept of imminence in light of little scholarly agreement on the issue); Bethlehem, *supra* note 3, at 773–74 ("There is little scholarly consensus on what is properly meant by 'imminence' in the context of contemporary threats."); Elizabeth Wilmshurst, *The Chatham House Principles of International Law on the Use of Force in Self-Defence*, 55 INT'L & COMP. L.Q. 963, 967–68 (2006) (suggesting that imminence is not merely a temporal criterion but depends on the nature of the threat).

104. Noam Lubell, *The Problem of Imminence in an Uncertain World*, *in* THE OXFORD HANDBOOK OF THE USE OF FORCE IN INTERNATIONAL LAW, *supra* note 16, at 697–98, 702–05.

105. ARSIWA, *supra* note 4, art. 25, para. 15.

106. Hung. v. Slovk., 1997 I.C.J. at 42, para. 54.

107. TALLINN MANUAL 2.0, *supra* note 1, at 138–39.

less certain and inevitable" that the harm will occur but where it is unclear when this will happen.[108]

This approach raises questions regarding the requisite degree of certainty that would justify uncoupling imminence from the requirement of temporal proximity. The overarching question is to what extent uncertainty should preclude a State from claiming the existence of a grave and imminent peril. On this point, *Tallinn Manual 2.0* quotes from the ILC commentary on Article 25 of the Articles on State Responsibility pursuant to which "a measure of uncertainty about the future does not necessarily disqualify a State from invoking necessity, if the peril is clearly established on the basis of the evidence reasonably available at the time."[109] Furthermore, it is stated in *Tallinn Manual 2.0* that "a State may only act when a reasonable State in the same or similar circumstances would act."[110] A standard based on reasonableness allows some degree of uncertainty as to whether sufficient harm will actually occur. Situations triggering the plea of necessity are often characterized by uncertainty, which can result from either the unpredictability of human behavior (Will a person finally take the decision to act in a harmful way?) or a lack of scientific knowledge or evidence (Will a particular substance in reaction with other substances actually have a damaging effect?). Caroline Foster has advanced the view that—based on the assumption that a peril may objectively exist even though there was no scientific evidence—imminence should be interpreted more generously in a situation of scientific uncertainty than in a situation where the damaging effect depended on the further actions of an individual.[111] The problem of uncertainty is highly relevant in the cyber domain since the purpose of a particular operation and the peril that it may pose cannot always be clearly identified at the time the incident is detected. Direct and short-term consequences of a cyber operation may be anticipated more easily than the long-term and collateral impact of such an incident. The infiltration of alien code into a computer system, for example, could just be a means of cyber espionage or the first step in a devastating cyber attack.[112] It might thus be completely unclear whether a cyber operation will result in further damage and, if so, whether this would happen automatically (like an attack with a logic bomb) or require additional steps to be taken by the author of the operation. Uncertainty about the nature of a malicious code is in some aspects comparable to scientific uncertainty. Advancing the argument that

108. Hung. v. Slovk., 1997 I.C.J. at 42, ¶ 54.

109. ARSIWA, *supra* note 4, art. 25, para. 16; *see also* TALLINN MANUAL 2.0, *supra* note 1, at 138 (referencing Article 25 of the Articles on State Responsibility as requiring decisions "clearly established on the basis of the evidence reasonably available").

110. TALLINN MANUAL 2.0, *supra* note 1, at 138.

111. Caroline Foster, *Necessity and Precaution in International Law: Responding to Oblique Forms of Urgency*, 23 N.Z. U. L. REV. 265, 282–83 (2008).

112. Geiß & Lahmann, *supra* note 11, at 647.

uncertainty in such cases also warrants a more generous interpretation of imminence (as suggested with a view to environmental necessity),[113] however, could seriously increase the risk of escalation of cyber conflict.

Instead of going down this path, *Tallinn Manual 2.0* introduces a standard according to which a peril is always imminent when the "window of opportunity" to take action is about to close.[114] The last window of opportunity standard is also familiar from the debate surrounding the right to anticipatory self-defense.[115] In the self-defense context it has been held that the "last feasible window" for anticipatory action, depending on the circumstances of the case, "may present itself immediately before" an attack or may open "long before."[116] The decisive question, according to this standard, is "whether a failure to act at that moment would reasonably be expected to result in the State being unable to defend itself effectively when that attack actually starts."[117] Noam Lubell described the "last window of opportunity" standard as "opening up a wider temporal framework with no regard to the immediacy of the threat."[118] In the words of Michael Schmitt, the standard combined the "requirement for a very high reasonable expectation" of a future attack with "an exhaustion of remedies component."[119] A similar approach has been discussed in the context of environmental necessity. Caroline Foster has argued that a peril should be treated as imminent "at the point when it appears reasonable for [the] State . . . to conclude, based on all the available scientific knowledge, that preventive action must be taken."[120] This view considers that ecological damage, while it may take years or even decades to manifest, at some stage can become irreversible. The last window of opportunity standard generally provides States with considerable leeway for action, whether invoking the right to self-defense or the plea of necessity. Even if the expected harm will realistically occur in the more distant future, reliance on the last window of opportunity standard makes it relatively easy for States to claim that early action was necessary to safeguard their essential interests because otherwise they would have risked losing the chance to effectively prevent the harm from occurring. Such a standard makes the plea of necessity particularly prone to

113. Foster, *supra* note 111, at 282–83.

114. TALLINN MANUAL 2.0, *supra* note 1, at 139.

115. *See, e.g.*, Vaughan Lowe, *'Clear and Present Danger': Responses to Terrorism*, 54 INT'L & COMP. L.Q. 185, 192 (2005) (describing the difficulty of applying the concept of imminence, as used in the traditional formulation of self-defense, to a hypothetical terrorist threat); Michael N. Schmitt, *Preemptive Strategies in International Law*, 24 MICH. J. INT'L L. 513, 534–35 (2003) (describing factors affecting a nation-state's choice to preemptively respond to a threat and proposing a legal standard based on the "*last possible window of opportunity*").

116. TALLINN MANUAL 2.0, *supra* note 1, at 351.

117. *Id.*

118. Lubell, *supra* note 104, at 710.

119. Schmitt, *supra* note 115, at 535.

120. Foster, *supra* note 111, at 277.

abuse. Apart from that, it is debatable whether the last window of opportunity standard actually reflects customary international law as far as the plea of necessity is concerned. And finally, further opening up the temporal framework of the plea of necessity has a significant impact not only on the prognosis concerning the likelihood and gravity of the peril but also on the evaluation of the sole means element. If the anticipated harm is still very far away in temporal terms, it may be harder to establish that its occurrence is sufficiently probable and that it will be sufficiently severe. In any case, the invoking State will have to substantiate thoroughly that the early action taken is really *the only way* to safeguard the endangered interest.[121]

IV. Towards a Special Necessity Regime for Cyber Incidents

This essay has started with a warning that an excessive and abusive invocation of the plea of necessity in response to cyber incidents might severely heighten the risk of escalation of inter-State conflict and, in the longer term, have a destabilizing effect on international peace and security. The contours of the concept of necessity as applied in the cyber context are not yet sufficiently clear to completely dispel these concerns. To lower the risk of escalation, States should develop a customized multilateral framework for resolving cyber incidents in situations that rise to the level of a state of necessity. Specifications of necessity at the level of primary rules can be found in many areas of international law. They may take the form of provisions (as contained in international human rights conventions or investment treaties) derogating in exigent circumstances from certain treaty obligations, but there are also special necessity regimes such as the *International Convention Relating to Intervention on the High Seas in Cases of Oil Pollution Casualties* of 1969.[122] This Convention was drafted and adopted shortly after the *Torrey Canyon* incident, which had shown quite plainly that there was an urgent need for regulating emergency responses in such cases. The Convention is focused on ensuring that states, when reacting to certain incidents defined in the Convention, follow standard procedures in order to minimize further harm. The obligations include diligent evaluation of the proportionality and necessity of the envisaged measures, consultation with other affected State and non-State parties, and notification of the measures to the affected parties and to relevant multilateral institutions.[123]

---

121. For a similar discussion in the context of self-defense, see Akande & Liefländer, *supra* note 103, at 564–65 (discussing the different relationships between necessity and imminence depending on the sort of attack to which a State is responding); Lubell, *supra* note 104, at 711–12 ("[T]he lack of imminence will most likely deliver a fatal blow to the credibility of an argument based on necessity."); *id.* at 716 (arguing that advancing along the temporal scale will reduce the likelihood of a future attack).

122. International Convention Relating to Intervention on the High Seas in Cases of Oil Pollution Casualties, Nov. 29, 1969, 970 U.N.T.S. 211.

123. *Id.* arts. III & V.

Special regard is paid to balancing the possible damage caused by the measures.[124] Moreover, the Convention contains provisions on compensation and dispute settlement.[125] These obligations may serve as a starting point to identify specific standards for dealing with situations of necessity in the cyber context.

To be clear, the point made here is not to refine due diligence obligations of states aimed at securing their own cyber infrastructure against malicious cyber activities. This field of regulation has already received considerable attention by scholars and practitioners.[126] The point is rather to establish due diligence obligations for States invoking the plea of necessity in the face of certain serious cyber incidents. At the U.N. level, several Groups of Governmental Experts (U.N. GGE) have already touched upon this issue, albeit in a very general way (due to the politically sensitive composition of the groups and the consensual nature of their reports).[127] Other relevant fora may include NATO, OSCE, the European Union, and the global Forum for Incident Response and Security Teams (FIRST).

Procedural norms that foster accountability and confidence building (e.g., provisions on consultation, information exchange, practical cooperation, the establishment of points of contact, and dispute settlement) are usually less controversial than substantive norms. But still, reaching a binding international agreement on such norms with a view to tackling certain serious and sensitive cyber incidents would be a complex, time-consuming and incalculable undertaking. A political code of conduct could therefore be a more practicable first step to promote relevant standards. The U.N. GGE report of 2015 recommends that States should consider voluntary, nonbinding norms, rules or principles of responsible behavior to reduce the risk of misperception, escalation, and conflict.[128] Inter alia, it is stipulated in the report that States should not use authorized emergency response teams to engage in malicious activity.[129]

It is not an unusual approach in the field of international lawmaking to start with formulating soft norms and urge States to commit to the norms by adapting their practices. At some point in the future, if and when States start to consider themselves legally bound by these norms, the process may result

---

124. *See id.* art. V (mandating that countries consider the damages caused by their proposed measures).

125. *Id.* arts. VI & VIII.

126. *See, e.g.*, TALLINN MANUAL 2.0, *supra* note 1, at 30–50 (discussing the due diligence obligations of a State to monitor infrastructure under its control to protect other States from cyber attacks using that infrastructure).

127. Group of Governmental Experts on Devs. in the Field of Info. and Telecomm. in the Context of Int'l Security, U.N. Doc. A/65/201 (July 30, 2010); U.N. Doc. A/68/98 (June 24, 2013); U.N. Doc. A/70/174 (July 22, 2015).

128. U.N. Doc. A/70/174, *supra* note 127, at 7–8.

129. *Id.* at 8.

in the evolution of new customary international law. Pressure from civil society and the business sector should not be underestimated in the process. These actors may be powerful drivers of an international effort to develop a functioning emergency regime for resolving cyber incidents at the inter-State level. After all, there are good reasons why States would want to pursue such an approach. On the one hand, each State may come into situations in which it has to resort to necessity to protect its essential interests against a grave and imminent peril posed by a cyber operation. On the other hand, each State may also face situations in which its rights are being breached by other States conducting active cyber defenses in the name of necessity. Taking into account the level of interconnectedness and interdependency as well as the growing importance of global cyber infrastructure, it should be presumed that States have a natural interest in resolving such incidents as swiftly and peacefully as possible. By adhering to adequate procedural standards, States could demonstrate that they are willing to act in good faith and not use the plea of necessity as a pretext for forcible action in the cyber domain when the right to self-defense and the law of countermeasures are not available.

Respect for Sovereignty in Cyberspace

Michael N. Schmitt* and Liis Vihul**

I. Discord Regarding Sovereignty

In the late 1990s, the international legal community's attention began to turn to a new form of warfare, then labeled "computer network attack," a type of information operations.[1] At the time, the Department of Defense (DoD) was at the cutting edge of thought regarding the legal significance of these operations. By 1999 its consideration of the issue had matured, and the Office of the General Counsel released *An Assessment of International Legal Issues in Information Operations*,[2] which considered the application of the *jus ad bellum* and *jus in bello* rules, space law, international telecommunication law, the law governing espionage activities, specific treaty regimes, and domestic law to military operations in cyberspace. *Information Operations* operated from the premise that international law applies in cyberspace. This remains the U.S. approach nearly two decades later.[3]

Yet, the document was cautionary. As it perceptively noted, the international legal system is reactive in the sense that it typically develops in

---

* Professor of International Law, University of Exeter; Chairman, Stockton Center for the Study of International Law, U.S. Naval War College; Francis Lieber Distinguished Scholar, Lieber Institute, U.S. Military Academy at West Point; Director, *Tallinn Manual 2.0* Project. The views expressed are those of the author in his personal capacity.

** CEO, Cyber Law International; Managing Editor, *Tallinn Manual 2.0* Project.

1. *See* JOINT CHIEFS OF STAFF, JOINT PUBL'N 3-13, JOINT DOCTRINE FOR INFORMATION OPERATIONS viii, GL-5 (1998), http://www.c4i.org/jp3_13.pdf [https://perma.cc/F6LP-T4UJ] (approving the addition of "computer network attack" to the Department of Defense Dictionary of Military and Associated Terms). Information operations are "[t]he integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own." JOINT CHIEFS OF STAFF, JOINT PUBL'N 1-02, DEPARTMENT OF DEFENSE DICTIONARY OF MILITARY AND ASSOCIATED TERMS 110 (2016), https://fas.org/irp/doddir/dod/jp1_02.pdf [https://perma.cc/7WWV-NHYK].

2. *See* U.S. Dep't of Def., Office of Gen. Counsel, *An Assessment of International Legal Issues in Information Operations* (2d ed. 1999), *in* COMPUTER NETWORK ATTACK AND INTERNATIONAL LAW 459, 463–65 (Michael N. Schmitt & Brian T. O'Donnell eds., 2002) [hereinafter *Information Operations*].

3. There appears to be near-universal consensus that the extant international law governs cyber activities. *See, e.g.*, Rep. of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, ¶ 24, U.N. Doc. A/70/174 (July 22, 2015) [hereinafter U.N. GGE 2015 Report] (reaffirming and expanding upon the 2013 Report *infra*); Rep. of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, ¶ 19, U.N. Doc. A/68/98 (June 24, 2013) [hereinafter U.N. GGE 2013 Report] (highlighting international law's significance for information and communications technologies).

response to particular situations and their consequences.[4] This being so, the assessment warned, "we can make some educated guesses as to how the international legal system will respond to information operations, but the direction that response actually ends up taking may depend a great deal on the nature of the events that draw the nations' attention to the issue."[5] Evolution in the law's interpretation in the cyber context was therefore inevitable.

What appears to have changed since then is the DoD's position on sovereignty in cyberspace. In 1999, the question was not whether a State could violate another State's sovereignty as a matter of law; rather, the challenge was identifying when cyber operations do so. That the prohibition on violation of sovereignty is a substantive rule of international law was an assumption that permeated the assessment. For example, it noted that in air law the entry by one State's aircraft into another's national airspace was "regarded as a violation of its sovereignty and territorial integrity."[6] In the maritime environment, the document pointed to the 1949 *Corfu Channel* case,[7] in which the International Court of Justice held that the penetration of Albanian territorial waters by British warships, and the minesweeping operation therein, without legal justification amounted to a violation of Albanian sovereignty.[8]

Regarding cyber operations, the document observed that "[a]n 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 . . . ."[9] And with respect to responding by cyber means against individuals or groups operating from other States, it noted that:

> [e]ven if it were possible to conduct a precise computer network attack on the equipment used by such individual actors, the state in which the effects of such an attack were felt, if it became aware of it, could well take the position that its sovereignty and territorial integrity had been violated.[10]

Thus, as framed in the 1999 DoD assessment, certain State cyber operations against other States might violate the latter's sovereignty, that is, constitute an "internationally wrongful act."[11] In the same vein, and over a

---

4. *Information Operations*, *supra* note 2, at 464.

5. *Id.* at 465.

6. *Id.* at 464.

7. *Id.* at 481.

8. Corfu Channel (U.K. v. Alb.), Judgment, 1949 I.C.J. Rep. 4, 36 (Apr. 9).

9. *Information Operations*, *supra* note 2, at 485.

10. *Id.* at 488.

11. An internationally wrongful act of a State consists of an action or omission that is attributable to the State under international law and constitutes a breach of an international

decade later, the premise of sovereignty as a primary rule of international law capable of being violated was accepted unanimously by the international law scholars and practitioners who prepared the 2013 *Tallinn Manual on the International Law Applicable to Cyber Warfare*, as well as those who produced its 2017 successor, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*.[12]

Recently, the DoD has indicated that it may have reassessed its position that sovereignty can be violated as a matter of international law in the cyber context. The prospect surfaced publicly in a panel presentation by Colonel Gary Corn, the Staff Judge Advocate of U.S. Cyber Command, at the 2016 "CyCon U.S." conference.[13] Then, on the day before the President's inauguration, Jennifer O'Connor, the Department's General Counsel, issued a memorandum titled "International Law Framework for Employing Cyber Capabilities in Military Operations" that dealt with, inter alia, the subject of sovereignty.[14]

Addressed to the Commanders of the Combatant Commands and very senior lawyers throughout the DoD, the memorandum was initially unclassified and circulated widely internationally. However, it was later designated as "for internal use only," and distribution is now restricted.[15] Nevertheless, Corn and former Principal Deputy General Counsel of the DoD Robert Taylor have since published on the subject.[16] Considering their positions as, respectively, the most senior legal advisor for the U.S. organization that engages in military cyber operations, the author of the memorandum, and a highly placed DoD attorney at the time it was issued, it

---

obligation of the State. G.A. Res. 56/83, annex, Responsibility of States for Internationally Wrongful Acts, art. 2 (Jan. 28, 2002) [hereinafter Articles on State Responsibility].

12. TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS 1 (Michael M. Schmitt & Liis Vihul eds., 2017) [hereinafter TALLINN MANUAL 2.0]; TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE (Michael N. Schmitt ed., 2013) [hereinafter TALLINN MANUAL 1.0]. Primary rules are those which impose either obligations or prohibitions on States. They must be distinguished from secondary rules of international law, that is, "the general conditions under international law for the State to be considered responsible for wrongful actions or omissions, and the legal consequences which flow therefrom." *Responsibility of States for Internationally Wrongful Acts*, [2001] 2 Y.B. Int'l L. Comm'n 31, U.N. Doc. A/CN.4/SER.A/2001/Add.1. Examples of secondary rules include those regarding attribution and the remedies that are available to States when international law obligations owed them are breached.

13. Colonel Corn was, however, speaking in his personal capacity. The authors spoke on the same panel.

14. Memorandum from Jennifer M. O'Connor, Gen. Counsel of the Dep't of Def., International Law Framework for Employing Cyber Capabilities in Military Operations (Jan. 19, 2017); *see infra* note 15 and accompanying text.

15. As one of the authors is a DoD employee, the document cannot be quoted in this article.

16. Gary Corn, *Tallinn Manual 2.0—Advancing the Conversation*, JUST SECURITY (Feb. 15, 2017) https://www.justsecurity.org/37812/tallinn-manual-2-0-advancing-conversation/ [https://perma.cc/T5XL-XK53]; Gary P. Corn & Robert Taylor, *Sovereignty in the Age of Cyber*, AM. J. INT'L L. UNBOUND (forthcoming).

is reasonable to assume that their views are consistent with the DoD's position.

By their approach, sovereignty does not operate as a rule of international law, the violation of which results in international legal responsibility.[17] Instead, it is a "baseline principle . . . undergirding binding norms,"[18] particularly the U.N. Charter Article 2(4) prohibition on the use of force and the customary international law prohibition on coercive intervention.[19] This article examines the point of contention between the DoD's earlier view, as well as the *Tallinn Manuals*', and that which now appears to be the revised DoD position. Part II assesses the legal logic underlying the argument against the existence of such a rule and sets forth the position of the authors on the matter. Drawing on the approach adopted in *Tallinn Manual 2.0*, it focuses on territorial sovereignty and its inviolability by other States. In Part III, evidence that the prohibition on violating sovereignty reflects customary international law is surveyed. Included are discussions of treatment of the matter by international tribunals, States, and international organizations. A brief illustration of how the two views might play out in practice is offered in Part IV, together with the authors' thoughts on the possible consequences of the debate.

II. Assessing the Argument Against a Primary Rule on Violations of Sovereignty

As noted, the authors of the two *Tallinn Manuals* unanimously agreed that the principle of sovereignty proscribes certain cyber operations conducted by States against other States. *Tallinn Manual 2.0* accordingly provides in Rule 4 that "[a] State must not conduct cyber operations that violate the sovereignty of another State."[20] Corn took issue with the substance of the rule in a *Just Security* post that followed publication of the *Manual* and was subsequently joined by Taylor in an *AJIL Unbound* piece further developing the position.[21]

Much of the argument they put forth is uncontroversial. For instance, both sides of the debate agree that the principle of sovereignty is the basis for the international law prohibitions of intervention and use of force.[22] Yet, advocates of the "sovereignty-as-principle-only" approach draw the line at these two internationally wrongful acts, rejecting any directly operative

17. Corn & Taylor, *supra* note 16.

18. Corn, *supra* note 16.

19. U.N. Charter art. 2, ¶ 4 ("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.").

20. TALLINN MANUAL 2.0, *supra* note 12, at 17 (Rule 4).

21. Corn, *supra* note 16; Corn & Taylor, *supra* note 16.

22. Corn & Taylor, *supra* note 16; TALLINN MANUAL 2.0, *supra* note 12, at 11–12.

effect of the principle itself, such as a rule prohibiting the breach of territorial inviolability. According to Corn and Taylor:

> [I]t is widely recognized that states have unquestioned authority to prohibit espionage within their territory under their domestic laws, but it is also widely recognized that international law does not prohibit espionage. States have long engaged in espionage operations that involve undisclosed entry and activities within the territory of other states, subject only to the risk of diplomatic consequences or the exercise of domestic jurisdiction over intelligence operatives if discovered and caught. Within this framework, it is understood that espionage may violate international law only when the modalities employed otherwise constitute a violation of a specific provision of international law, such as an unlawful intervention or a prohibited use of force. Thus states conduct intelligence activities in and through cyberspace, and generally, "to the extent that cyber operations resemble traditional intelligence and counter-intelligence activities . . . such cyber operations would likely be treated similarly under international law." This framework applies equally to cyber operations directed at terrorist cyber infrastructure located within the territory of another state.
>
> Further, the differences in how sovereignty is reflected in international law with respect to the domains of space, air, and the seas further supports the view that sovereignty is a principle, subject to adjustment depending on the domain and the practical imperatives of states rather than a hard and fast rule. For instance, in the case of the space domain, objects in orbit are beyond the territorial claims of any nation, and outer space – including outer space above another state's territory – is available for exploitation by all. In the case of the air domain, the regime is highly restrictive, such that any unconsented entry into the airspace of another state is regarded as a serious violation of international law subject to such exceptions as self-defense, Security Council authorization, or force majeure. In the case of the seas, many entries into and travels through the territory of another state are permissible without the consent of that state, but there are conditions under which such entry would be a violation of international law – it depends on the particular facts and circumstances. The fact that states have developed vastly different regimes to govern the air, space, and maritime domains underscores the fallacy of a universal rule of sovereignty with a clear application to the domain of cyberspace. The principle of sovereignty is universal, but its application to the unique particularities of the cyberspace domain remains for states to determine through state practice and/or the development of treaty rules.[23]

23. Corn & Taylor, *supra* note 16 (emphasis omitted).

This is where their argument breaks down, for it fails to recognize that each of the legal regimes cited—air, space, maritime, and that governing espionage—are premised on territorial integrity and inviolability. Regarding the air domain, consider a Russian military aircraft that briefly "cuts the corner" into Estonian airspace. There is no State practice supporting treatment of these incidents, which are the subject of the ongoing NATO Baltic Air Policing mission, as a use of force or coercive intervention.[24] On the contrary, they constitute violations of Estonian national airspace,[25] and thereby its territorial sovereignty. As will be seen, this is the generally consistent approach States take to aerial intrusions into inviolable national airspace.[26]

With respect to outer space, States have confirmed in treaty law that it is not subject to national appropriation by claim of sovereignty.[27] This indicates that but for that rule, which is now accepted as customary in nature, territorial sovereignty would by default be viewed as extending beyond the airspace above a State's sovereign territory into outer space. Space law is therefore *lex specialis* that allows, for instance, States to place space objects into geostationary orbit above the subjacent territory of other States.[28] It is a legal accommodation agreed to by States that is designed to permit them to operate in outer space in ways that might otherwise be prohibited through application of the *lex generalis* rules of territorial sovereignty.

The law of the sea also supports the primary-rule status of territorial sovereignty. Recall that Corn and Taylor opine, in reference to maritime activities, that "many entries into and travels through the territory of another

---

24. *See NATO Air—Policing Mission*, LITHUANIAN ARMED FORCES, https://kariuomene.kam.lt/en/structure_1469/air_force/nato_air_-_policing_mission.html [https://perma.cc/E82T-QQT8] (updated Mar. 1, 2017) ("NATO allies provided 34 rotations of air capabilities to patrol the Baltic airspace over the span of the mission . . . to fill in the Baltic States' shortage of relevant aircraft for independent protection of national airspace.").

25. *See, e.g.*, *Estonia Says Russian Aircraft Violated Airspace Again*, RADIO FREE EUROPE/RADIO LIBERTY (Sept. 6, 2016), http://www.rferl.org/a/russia-estonia-airspace-violated/27970888.html [https://perma.cc/9JCW-3A3Q] (recounting the Estonian military's claim that a Russian aircraft violated Estonian airspace by flying within it "without permission for about 90 seconds").

26. The Chicago Convention provides, "The contracting States recognize that every State has complete and exclusive sovereignty over the airspace above its territory." Convention on International Civil Aviation, art. 1, Dec. 7, 1944, 61 Stat. 1180, 15 U.N.T.S. 295. Use of the term "recognize" confirms the customary international law character of such sovereignty.

27. Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies, art. II, Jan. 27, 1967, 18 U.S.T. 2410, 610 U.N.T.S. 205.

28. *See, e.g.*, Definition and Delimitation of Outer Space and the Character and Utilization of the Geostationary Orbit, 2001 DIGEST OF UNITED STATES PRACTICE IN INTERNATIONAL LAW, ch. 12, § C(4) at 722 ("Article II . . . further states that outer space is not subject to national appropriation by claim of sovereignty or by any other means. Thus, a signatory . . . cannot appropriate a position in the [geostationary orbit] either by claim of sovereignty or by means of use, or even repeated use, of such an orbital position.").

State are permissible without the consent of that State, but there are conditions under which such entry would be a violation of international law—it depends on the facts and circumstances."[29] While their statement of the law is correct, the authors fail to acknowledge the reason why consent of the coastal States need not be obtained when another State's vessel wishes to sail through the former's territorial sea. States have long enjoyed territorial inviolability vis-à-vis their coastal waters. The regimes of innocent, transit, and archipelagic passage developed as customary and treaty-law exceptions to the territorial sea's inviolability;[30] they modify the baseline principle that maritime borders may not be pierced by other States.[31] Territorial inviolability remains intact, subject to the exceptions.

Finally, the issue of espionage can also be viewed through the prism of territorial sovereignty. Corn and Taylor point to the long-standing State practice of engaging in espionage activities on foreign territory, which they suggest is not viewed by States as a violation of international law.[32] Although they do not set forth the legal basis for this conclusion, a plausible argument supporting it is that, based on the extensive State practice of conducting espionage abroad, espionage constitutes a customary exception to the general rule that territorial sovereignty is inviolable. The weakness in this rationale is the limited amount of *opinio juris* on point, for a new customary international law rule must be grounded in both State practice and *opinio juris*.

By the opposing view, espionage on another State's territory is de jure a violation of that State's territorial sovereignty.[33] For those advocating this position, the question in the case of remotely conducted cyber-espionage operations, therefore, would be identical to that which must be asked of any other cyber operation—at what point does an operation that does not entail physical presence on another State's territory qualify as a violation of territorial sovereignty? The manner in which the *Tallinn Manual 2.0* answers this question is set out below. But irrespective of which side of the debate

---

29. Corn & Taylor, *supra* note 16.

30. United Nations Convention on the Law of the Sea, arts. 17, 38, 52, 53, Dec. 10, 1982, 1833 U.N.T.S. 397 [hereinafter Law of the Sea Convention].

31. This conclusion is without prejudice to authorization or mandate by the U.N. Security Council under Chapter VII of the U.N. Charter, operations conducted pursuant to the right of self-defense, or situations provided for in the law of the sea, such as *force majeure* or distress. *See* U.N. Charter arts. 42 (providing the basis for "peace enforcement" operations), 51 (affirming the right of self-defense); Law of the Sea Convention, *supra* note 30, art. 18, ¶ 2 (allowing stopping and anchoring in territorial seas as rendered necessary by exigent circumstances).

32. Corn & Taylor, *supra* note 16.

33. *See, e.g.*, TALLINN MANUAL 2.0, *supra* note 12, at 18–19, 171 (noting that "[i]n the cyber context . . . it is a violation of territorial sovereignty for an organ of a State, or others whose conduct may be attributed to the State, to conduct cyber operations while physically present on another State's territory," and suggesting the majority view is that cyber espionage would constitute violation of sovereignty if the individual committing the espionage operation "is on another State's territory while nonconsensually engaging in the operation").

one takes, territorial sovereignty resides at the heart of the underlying legal logic.

To bolster their position on territorial sovereignty, Corn and Taylor turn to the work of scholars, principally Ian Brownlie's classic work, *International Law*.[34] It is true that Brownlie characterizes the term "sovereignty" as "rather descriptive in character, referring in a 'catch-all' sense to the collection of rights held by a state."[35] What they fail to note, however, is that Brownlie, citing *Corfu Channel*, undeniably sees territorial inviolability as one of those rights and observes that other States accordingly shoulder a "correlative duty of respect for territorial sovereignty."[36]

The seminal treatise in the field, Lassa Oppenheim's *International Law*, also endorses the notion that territorial sovereignty must be respected and that failure to do so constitutes a violation of international law. This view was advanced in the book's first edition, published in 1905.

> The duty of every State to abstain itself and to prevent its organs and subjects from any act which contains a violation of another State's independence or territorial and personal supremacy is correlative to the respective right of the other State. It is impossible to enumerate all such actions as might contain a violation of this duty. But it is of value to give some illustrative examples. . . . Further, in the interest of the territorial supremacy of other States, a State is not allowed to send its troops, its men-of-war, and its police forces into or through foreign territory, or to exercise an act of administration or jurisdiction on foreign territory, without permission.[37]

It has stood the test of time, for, although revised to accommodate new factual circumstances and the maturation of international law, the analysis was maintained by each of the book's distinguished subsequent editors.[38] The most recent edition (9th), published in 1992, provides,

---

34. Corn & Taylor, *supra* note 16.

35. JAMES CRAWFORD, BROWNLIE'S PRINCIPLES OF PUBLIC INTERNATIONAL LAW 448 (8th ed. 2012).

36. *Id.*; *see also* James Crawford, *Sovereignty as a Legal Value*, *in* INTERNATIONAL LAW 117, 121 (James Crawford & Martti Koskenniemi eds., 2012) ("As a general matter, [sovereign] authority is exclusive: normally, governmental activity carried out on the territory of another state is only lawful if performed there with the latter's consent . . . ."); H.W. HALLECK, INTERNATIONAL LAW 270 (1861) ("Every right has its correlative duty," which in the present context would mean that a State's right to exclusive authority within its territory carries with it the correlative duty to respect the same right of other States); MALCOLM N. SHAW, INTERNATIONAL LAW 353 (7th ed. 2014) ("The principle of respect for the territorial integrity of states is well founded as one of the linchpins of the international system, as is the norm prohibiting interference in the internal affairs of other states.").

37. LASSA OPPENHEIM, 1 INTERNATIONAL LAW: PEACE 172–73 (1905).

38. R.F. Roxburgh, Lord Arnold McNair, Sir Hersch Lauterpacht, Sir Robert Jennings, and Sir Arthur Watts.

> All states are under an international legal obligation not to commit any violation of the independence, or territorial or personal authority, of any other state.
>
> . . . .
>
> It is not feasible to enumerate all such actions as might constitute a breach of a state's duty not to violate another state's independence or territorial or personal authority. But it is useful to give some illustrative examples. . . . A state is not allowed to send its troops, its warships, or its police forces into or through foreign territory, or its aircraft over it, or to carry out official investigations on foreign territory or to let its agents conduct clandestine operations there, or to exercise an act of administration or jurisdiction on foreign territory, without permission.[39]

As is apparent, it is misguided to assert that there must exist a cyber-specific rule for cyber operations not amounting to a wrongful use of force or coercive intervention, but manifesting on another State's territory, to qualify as violations of territorial sovereignty. The pressing task is, instead, to identify the criteria for violation thereof by means of cyber operations. Only if *lex specialis* subsequently emerges through treaty or crystallization of customary law, as in the case of outer space, will cyber operations that would otherwise violate a State's territorial sovereignty be permissible.

Treating violations of sovereignty as a primary rule of international law, *Tallinn Manual 2.0* seeks to add granularity to the circumstances in which a cyber operation might violate a State's territorial sovereignty. The commentary to Rule 4, set out above, provides that, as a general matter, "[c]yber operations that prevent or disregard another State's exercise of its sovereign prerogatives constitute a violation of such sovereignty and are prohibited by international law."[40] States enjoy sovereignty over cyber infrastructure, persons, and cyber activities located on their territory.[41] This includes both public and private cyber infrastructure.[42]

For the experts who produced *Tallinn Manual 2.0*, the difficulty lay in identifying those cyber operations that would violate it. They conducted their analysis along two axes: "(1) the degree of infringement upon the target

---

39. 1 OPPENHEIM'S INTERNATIONAL LAW: PEACE 382, 385–86 (Robert Jennings & Arthur Watts eds., 9th ed. 1992) [hereinafter OPPENHEIM'S INTERNATIONAL LAW].

40. TALLINN MANUAL 2.0, *supra* note 12, at 17.

41. *Id.* at 13 (Rule 2).

42. *Id.* at 13–14. This is without prejudice to exceptions provided for in law, such as diplomatic protection. *See, e.g.*, *id.* at 209 ("'Premises of a mission' refers to 'the buildings or parts of buildings and the land ancillary thereto, irrespective of ownership, used for the purposes of the mission.'") (quoting Vienna Convention on Diplomatic Relations, art. 1(i), Apr. 18, 1961, 23 U.S.T. 3227, 500 U.N.T.S. 95); *id.* at 212 ("Cyber infrastructure on the premises of a diplomatic mission or consular post is protected by the inviolability of that mission or post.").

State's territorial integrity; and (2) whether there has been an interference with or usurpation of inherently governmental functions."[43]

With respect to infringement on territorial integrity, there was consensus that a State's cyber operation causing physical damage or injury on the territory of another State violates the latter State's territorial sovereignty. The group also concurred that a cyber operation resulting in a loss of functionality (such that the targeted cyber infrastructure or the equipment upon which it relies needs to be repaired or replaced) qualifies as a violation. No consensus could be achieved, however, as to remote cyber operations generating other consequences. Some experts treated the aforementioned consequences as the threshold for violation. Others suggested that violations of sovereignty might include additional operations but were unable to agree upon a definitive threshold to apply.[44]

Clearly, however, not all cyber operations that manifest, either partially or totally, on another State's cyber infrastructure infringe that State's territorial inviolability.[45] As an example, the transmission of propaganda by one State into other States from platforms in outer space or on the high seas is not considered to violate sovereignty, even when done against the target States' wills.[46] The examples cited by Corn and Taylor would generally fall into this category. It is correct that cyber operations involving "cyber effects in, yet invisible to, the territorial State, but that only manifest operationally in the area of hostilities"[47] are generally permissible. Similarly, "[w]here the proposed cyber action is focused solely against the individual accounts or facilities of terrorists or terrorist organizations widely recognized as such, and when the cyber actions will generate only *de minimis* effects on nonterrorist infrastructure within the host State, international law does not preclude those cyber actions."[48] Yet, citing select examples of cyber operations that States are unlikely to consider violations of territorial sovereignty does not disprove the existence of a primary rule prohibiting breaches of territorial inviolability in other cases. On the contrary, it demonstrates the need to develop interpretive criteria by which that rule will be applied.

Tallinn Manual 2.0 additionally notes that a violation of sovereignty occurs whenever a cyber operation interferes with or usurps another State's inherently governmental functions.[49] This is the natural consequence of the

---

43. *Id.* at 20.

44. *Id.* at 20–21.

45. *See* OPPENHEIM'S INTERNATIONAL LAW, *supra* note 39, at 385 ("However, not all acts performed by one state in the territory of another involve a violation of sovereignty.").

46. BRUCE A. HURWITZ, THE LEGALITY OF SPACE MILITARIZATION 29–30 (1986).

47. Corn & Taylor, *supra* note 16.

48. *Id.* at 7.

49. TALLINN MANUAL 2.0, *supra* note 12, at 21. The experts found it difficult to define "inherently governmental functions" with granularity. *Id.* at 22. However, certain functions plainly

fact that, pursuant to the notions of internal and external sovereignty,[50] these functions fall within the exclusive purview of the State. Such violations need not be accompanied by any damage or injury, and unlike the prohibition on intervention into a State's *domaine réservé*, no coercive intent or effect is required. However, as the focus of the debate over sovereignty is on its territorial aspect, the discussion that follows shall be limited to territorial sovereignty and its inviolability.

The *Tallinn Manual 2.0* approach to sovereignty appears to be widely shared. Little criticism of the "sovereignty-as-rule" position, which was also reflected in the first edition of the *Tallinn Manual*,[51] was heard during the nearly four years between publication of the two editions. On the contrary, discussion of sovereignty in the cyber context surrounded the identification of those cyber activities that might violate another State's sovereignty.

Additionally, a draft of the *Tallinn Manual 2.0* rule on violation of sovereignty and its accompanying commentary was discussed in three meetings of over fifty States and international organizations that were convened by the Dutch Ministry of Foreign Affairs in 2015 and 2016.[52] Many of the States subsequently provided voluminous unofficial written comments. They voiced no meaningful objection to Rule 4. Instead, the comments focused on application of the rule to specific situations. There was even consideration of whether the prohibition encompassed cyber activities by non-State groups, a view acknowledged, but not accepted, in the *Manual*.[53] Throughout this process, it appeared to be received knowledge that a primary rule on territorial-sovereignty violations existed and applied to cyber operations.

III. Evidence of a Primary Rule on Violations of Sovereignty

The question at hand is whether the principle of sovereignty operates as a primary rule of customary international law, imposing an obligation on States to respect the inviolability of other States' territories.[54] If so, it

---

qualify. For example, law enforcement is a function reserved to the State alone. Accordingly, if one State conducts law enforcement by cyber means, such as remote electronic search, on another State's territory without the latter's consent, a violation of sovereignty has taken place.

50. *Id.* at 13 (Rule 2); *id.* at 16 (Rule 3).

51. TALLINN MANUAL 1.0, *supra* note 12.

52. Michael Schmitt, *The Tallinn Manual 2.0 on the International Law of Cyber Operations: What It Is and Isn't*, JUST SECURITY (Feb. 9, 2017), https://www.justsecurity.org/37559/tallinn-manual-2-0-international-law-cyber-operations/ [https://perma.cc/5YRS-F5TB].

53. TALLINN MANUAL 2.0, *supra* note 12, at 18.

54. Customary international law is described in the Statute of the International Court of Justice as "a general practice accepted as law." Statute of the International Court of Justice art. 38(1)(b), June 26, 1945, 59 Stat. 1031, 33 U.N.T.S. 993 [hereinafter ICJ Statute]. "Crystallization" of customary international law requires two elements—State practice (*usus*) and the conviction that said practice is engaged in, or refrained from, out of a sense of legal obligation (*opinio juris*). Continental Shelf (Libyan Arab Jamahiriya v. Malta), Judgment, 1985 I.C.J. Rep. 13, ¶ 27 (June 3)

imposes significant operational limits on State activities on, or with effects in, the territory of those States.

In the view of the authors, overwhelming evidence of State practice and *opinio juris*—the foundational elements of customary international law—supports the assertion that a primary rule not to violate the territorial sovereignty of other States exists. Examples of such practice and *opinio juris* are offered below. Additionally, pursuant to Article 38(1)(d) of the Statute of the International Court of Justice, "judicial decisions and the teachings of the most highly qualified publicists of the various nations" constitute "subsidiary means for the determination of rules of law."[55] Since judicial decisions, in particular those of the International Court of Justice, are especially persuasive subsidiary means for assessing whether a customary law rule has crystallized,[56] the examination of the supporting evidence begins with an appraisal of a number of key cases. As to the work of highly qualified publicists (scholars), the scholarship cited earlier self-evidently qualifies as such. Significant in the cyber context are the two *Tallinn Manuals*, the collective work of nearly forty scholars, many of whom are internationally renowned. They too would meet the requirements of Article 38(1)(d).[57] Although length constraints preclude a comprehensive catalogue of support for the existence of a primary rule on sovereignty, that which is set forth below is proffered regarding the substance of the norm as well as to indicate the breadth and depth of the corroborating evidence.

A. Judicial Treatment

The premise that it is unlawful for a State to act on the territory of another State without the latter's consent has long been recognized by international tribunals. In the 1927 *Lotus Case*, the Permanent Court of International Justice observed that "the first and foremost restriction imposed by international law upon a State is that—failing the existence of a permissive rule to the contrary—it may not exercise its power in any form in

("It is of course axiomatic that the material of customary international law is to be looked for primarily in the actual practice and *opinio juris* of States . . . ."). The classic case addressing these requirements is North Sea Continental Shelf (Ger. v. Den.; Ger. v. Neth.), Judgment, 1969 I.C.J. Rep. 3 (Feb. 20). For further discussion, see INT'L LAW ASS'N, COMM. ON FORMATION OF CUSTOMARY (GEN.) INT'L LAW, STATEMENT OF PRINCIPLES APPLICABLE TO THE FORMATION OF GENERAL CUSTOMARY INTERNATIONAL LAW ¶ 10 (2000); Yoram Dinstein, *The Interaction Between Customary International Law and Treaties*, *in* RECUEIL DES COURS 322 (2006).

55. ICJ Statute, *supra* note 54, art. 38(1)(d).

56. Michael Wood (Special Rapporteur), Int'l Law Comm'n, First Report on Formation and Evidence of Customary International Law, U.N. Doc. A/CN.4/663, at 21 (May 17, 2013); INT'L LAW ASS'N, *supra* note 54, at 4, 19.

57. ICJ Statute, *supra* note 54, art. 38(1)(d); *see* TALLINN MANUAL 2.0, *supra* note 12, at xii–xxii (listing scholars from various nations contributing to both the *Tallinn Manual 2.0* and *Tallinn Manual 1.0*).

the territory of another State."[58] In other words, the court treated the principle as one that sets binding limits on a State's activities on foreign territory; when a State acts without the territorial State's consent, the former is in breach of an obligation owed the latter to respect its sovereignty.

This view of the law has been adopted by the Permanent Court's successor, the International Court of Justice. Indeed, in its first case, *Corfu Channel*, the court dealt with accusations of violations of sovereignty.[59] The case involved an incident in which British warships passing through the Corfu Channel in Albanian territorial waters in 1946 struck naval mines.[60] Following the incident, the Royal Navy again sailed through the waters, this time to conduct minesweeping operations.[61] The United Kingdom sought a finding that Albania was responsible for the damage to two of its vessels and the ensuing loss of life, and an order that it pay compensation.[62] Albania counterclaimed, asking the court to decide whether the "United Kingdom under international law violated the sovereignty of the Albanian People's Republic by reason of the acts of the Royal Navy in Albanian waters," and, if so, whether there was a duty to provide satisfaction.[63]

The court held Albania responsible for the damage and loss of life on the basis that it had failed to warn the United Kingdom of the dangers posed by transit through the Corfu Channel.[64] More important to the territorial-sovereignty issue were the findings of the court relative to Albania's claim. The United Kingdom did not contest Albania's sovereignty over the waters, nor did it suggest the absence of a norm precluding violations of sovereignty. Instead, it argued that a special maritime legal regime, innocent passage, allowed for transit through international straits lying in a State's territorial sea, even in the absence of consent.[65] The court agreed and therefore was "unable to accept the Albanian contention that the Government of the United Kingdom ha[d] violated Albanian sovereignty by sending the warships through the Strait without having obtained the previous authorization of the Albanian Government."[66] The waters were subject to territorial sovereignty, but an exception applied.

---

58. S.S. "Lotus" (Fr. v. Turk.), Judgment, 1927 P.C.I.J. (ser. A) No. 10, at 18 (Sept. 7).

59. U.K. v. Alb., 1949 I.C.J. at 6.

60. *Id.* at 12–13.

61. *Id.* at 13.

62. *Id.* at 10–11.

63. *Id.* at 6.

64. *Id.* at 23.

65. *Id.* at 27. As it is an international strait, under the modern law of the sea, passage through the Corfu Channel would be "transit passage." Law of the Sea Convention, *supra* note 30, arts. 37–38.

66. U.K. v. Alb., 1949 I.C.J. at 29–30.

An opposite conclusion was reached with respect to the minesweeping. Because the operations were conducted without Albania's consent, and no exception operated, the court concluded that:

> Between independent States, respect for territorial sovereignty is an essential foundation of international relations. The Court recognizes that the Albanian Government's complete failure to carry out its duties after the explosions, and the dilatory nature of its diplomatic notes, are extenuating circumstances for the action of the United Kingdom Government. But to ensure respect for international law, of which it is the organ, the Court must declare that the action of the British Navy co[n]stituted a violation of Albanian sovereignty.[67]

Since the 1949 *Corfu Channel* judgment, the International Court of Justice has continued to address the issue of, and often find, internationally wrongful violations of sovereignty. In 1973, it considered the legality of French atmospheric nuclear testing in the South Pacific.[68] The case, *Nuclear Tests*, involved an Australian request for a declaratory judgment that the French testing violated international law, as well as a permanent order prohibiting France from carrying out further tests.[69] Although it was dismissed on procedural grounds, what is relevant to the issue of breach of sovereignty as a primary rule is the Australian government's position that the "deposit of radio-active fall-out on the territory of Australia and its dispersion in Australia's airspace without Australia's consent . . . violates Australian sovereignty over its territory."[70]

In its Memorial, Australia set forth its legal logic in making the claim:

> The Government of Australia repeats that its case rests upon several bases: on the mere fact of trespass, on the harmful effects associated with trespass, and on the impairment of its independent right to determine what acts shall take place within its territory. In this connection, the Government of Australia wants to emphasize that the mere fact of trespass, the harmful effects which flow from such fall-out and the impairment of its independence, each clearly constitute a violation of the affected State's sovereignty over and in respect of its territory.[71]

The court then addressed the issue of a legal right to allege a violation of sovereignty.

> The evident character of Australia's legal interest in a claim alleging violation of its sovereignty over and in respect of its territory is such

---

67. *Id.* at 35.

68. Nuclear Tests (Austl. v. Fr.), Judgment, 1974 I.C.J. Rep. 253, 254 (Dec. 20).

69. *Id.* ¶ 26.

70. Application, Nuclear Tests (Austl. v. Fr.), 1973 I.C.J. Pleadings 1, ¶ 49(ii)(a) (May 9).

71. Memorial of Australia, Nuclear Tests (Austl. v. Fr.), 1974 I.C.J. Pleadings 249, ¶ 454 (Nov. 23).

> as to make any extended argument upon this point superfluous. It is, indeed, quite obvious that a State possesses a legal interest in the protection of its territory from any form of external harmful action, as well as in the defence of the well-being of its population and in the protection of national integrity and independence. It would indeed be positively absurd to suggest otherwise. If a State did not possess a legal interest in such matters, how could Portugal have brought the *Naulilaa* case against Germany . . . ; how could Albania have brought against the United Kingdom in the *Corfu Channel* case . . . the claim arising out of the sweeping of mines in Albanian territorial waters? The point does not require elaboration.[72]

At least from the Australian perspective, even unintentional effects manifesting on its territory sufficed to breach territorial inviolability.

The International Court of Justice again faced the issue of territorial sovereignty in its 1986 *Nicaragua* judgment.[73] The case involved Nicaragua's assertion that the United States had breached its obligations under "general and customary international law" and "violated and is violating the sovereignty of Nicaragua" by "armed attacks against Nicaragua by air, land and sea"; "incursions into Nicaraguan territorial waters"; "aerial trespass into Nicaraguan airspace"; and "efforts by direct and indirect means to coerce and intimidate the Government of Nicaragua."[74]

When considering these claims, the court acknowledged linkage between State sovereignty and the prohibitions of the use of force and coercive intervention, but unambiguously differentiated between them, noting that a single act may violate more than one of the prescriptive norms:

> The effects of the principle of respect for territorial sovereignty inevitably overlap with those of the principles of the prohibition of the use of force and of nonintervention. Thus the assistance to the *contras*, as well as the direct attacks on Nicaraguan ports, oil installations, etc., . . . not only amount to an unlawful use of force, but also constitute infringements of the territorial sovereignty of Nicaragua, and incursions into its territorial and internal waters. Similarly, the mining operations in the Nicaraguan ports not only constitute breaches of the principle of the nonuse of force, but also affect Nicaragua's sovereignty over certain maritime expanses. The Court has in fact found that these operations were carried on in Nicaragua's territorial or internal waters or both . . . and accordingly they constitute a violation of Nicaragua's sovereignty. The principle of respect for territorial sovereignty is also directly infringed by the

72. *Id.* ¶ 456.

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

74. *Id.* ¶ 250.

> unauthorized overflight of a State's territory by aircraft belonging to or under the control of the government of another State.[75]

In the opinion of the court, then, territorial sovereignty enjoys independent valence. Indeed, it felt obligated to apprise the facts based on the "duty of every State to respect the territorial sovereignty of others."[76] Ultimately, the court found that the United States, through various actions, breached obligations under customary law with respect to intervention, use of force, and violation of territorial sovereignty.[77] In doing so, it treated violation of territorial sovereignty as a self-standing primary norm with no less normative force than the other two.

In 2015, the International Court of Justice examined Costa Rica's allegations that Nicaragua had sent armed forces into Costa Rican territory and dug a channel thereon, and Nicaragua's contentions that Costa Rica had built a road in the contested area and caused transboundary environmental damage to Nicaragua.[78] Both sides claimed that these actions violated their respective sovereignties. They disputed their opponent's claims on the basis that no violation had occurred because the other side did not enjoy sovereignty over the areas in question. Extracts from the judgment exemplify the legal argumentation of the two States:

> Costa Rica alleges that Nicaragua violated its territorial sovereignty in the area of Isla Portillos in particular by excavating in 2010 a *caño* with the aim of connecting the San Juan River with the Harbor Head Lagoon and laying claim to Costa Rican territory. According to Costa Rica, this violation of sovereignty was exacerbated by Nicaragua's establishment of a military presence in the area and by its excavation in 2013 of two other *caños* located near the northern tip of Isla Portillos.[79]
>
> . . . .
>
> Nicaragua does not contest that it dredged the three *caños*, but maintains that "Nicaragua enjoys full sovereignty over the *caño* joining Harbor Head Lagoon with the San Juan River proper, the right bank of which constitutes the land boundary as established by the 1858 Treaty . . . ." Nicaragua further submits that "Costa Rica is under an obligation to respect the sovereignty and territorial integrity

75. *Id.* ¶ 251.

76. *Id.* ¶ 213.

77. *Id.* ¶ 292.

78. Certain Activities Carried out by Nicaragua in the Border Area (Costa Rica v. Nicar.) and Construction of a Road in Costa Rica Along the San Juan River (Nicar. v. Costa Rica), Judgment, 2015 I.C.J. Rep. 1, 2–4 (Dec. 16), http://www.icj-cij.org/docket/files/150/18848.pdf [https://perma.cc/5RWF-RS9U].

79. *Id.* ¶ 66.

> of Nicaragua, within the boundaries delimited by the 1858 Treaty of Limits . . . ."[80]

For its part, the court adopted the same territorial sovereignty-based line of analysis. As an example, it observed, "[s]ince it is uncontested that Nicaragua conducted certain activities in the disputed territory, it is necessary, in order to establish whether there was a breach of Costa Rica's territorial sovereignty, to determine which State has sovereignty over that territory."[81] After answering that question, it unanimously found that "by excavating three *caños* and establishing a military presence on Costa Rican territory, Nicaragua has violated the territorial sovereignty of Costa Rica."[82]

In fact, the court left no room for debate regarding whether sovereignty can be violated as a matter of international law; it employed classic terms and concepts from the law of State responsibility, including "breach," "responsible for breach," and "obligation to make reparation," thereby affirming that the obligation to respect territorial sovereignty is legally binding.[83] Moreover, because the court found that Nicaragua had violated Costa Rica's sovereignty, it held that it did not have to determine whether Nicaragua's conduct amounted to a breach of the prohibition on the threat or use of force under the U.N. Charter or the Charter of the Organization of American States.[84] Finally, the court also noted that its determination that Nicaragua had breached the territorial sovereignty of Costa Rica "provides adequate satisfaction for the nonmaterial injury suffered on this account."[85]

At no time in the case did either party assert the absence of a primary rule prohibiting violations of sovereignty. On the contrary, that rule lay at the heart of both sides' claims. Nor did the court consider that option. All involved took the rule's existence as a normative given, and the court rendered its judgment on that basis.

B. State Practice and Opinio Juris

Unlike judicial decisions, State practice and expressions of *opinio juris* are obligatory elements of any claim that an obligation to respect sovereignty is legally binding in customary international law. In this regard, it must be noted that States sometimes act in ways that affect, but do not violate, the exercise of sovereign rights of other States, such as imposing sanctions that

---

80. *Id.* ¶ 68.

81. *Id.* ¶ 69.

82. *Id.* ¶ 229.

83. "These activities were in breach of Costa Rica's territorial sovereignty. Nicaragua is responsible for these breaches and consequently incurs the obligation to make reparation for the damage caused by its unlawful activities . . . ." *Id.* ¶ 93.

84. *Id.* ¶¶ 96–99.

85. *Id.* ¶ 139.

impact another State's domestic economic activities.[86] Additionally, the term "sovereignty" frequently appears in political statements without necessarily carrying legal weight. Thus, it is essential to be sensitive to customary law's formal components of State practice and *opinio juris* when examining what States do, how they react to actions by other States, and what their officials say publicly. The examples that follow have been carefully selected as illustrations of the way in which States treat the issue of sovereignty in international law, rather than as an international relations concept.

States have characterized a plethora of incidents as violations of their territorial sovereignty.[87] It must be cautioned that some involved the armed forces and therefore may also have implicated the prohibitions of the use of force or coercive intervention. The fact that States at times chose to discuss an incident as a breach of their territorial inviolability when the actions might also have crossed the use-of-force or coercive-intervention thresholds demonstrates that States consider the former to be a primary rule distinct from other primary rules that are based in the principle of sovereignty.

Unconsented-to aerial intrusions have long been considered a violation of the subjacent State's territorial sovereignty. Noteworthy in this regard is the incident involving the downing of an unarmed American U-2 reconnaissance aircraft by the Soviet Union and the capture of its pilot in 1960.[88] The United States did not protest the shoot-down. This reaction contrasts sharply with U.S. condemnation of the downing of an RB-47 reconnaissance aircraft by Soviet fighters and the imprisonment of its crew the same year.[89]

The difference can only be explained by virtue of the locations of the aircraft at the time of the shoot-downs, since both incidents involved military aircraft performing similar missions in the same year. In the case of the U-2, the aircraft was in Soviet national airspace, which both sides appeared to acknowledge was subject to Soviet sovereignty.[90] By contrast, the RB-47 was flying in what the United States characterized as international airspace above the high seas.[91] Accordingly, while the former involved a violation of

---

86. *See* André Beirlaen, *Economic Coercion and Justifying Circumstances*, 18 REVUE BELGE DE DROIT INT'L 57, 67–69 (1984) (discussing the line that demarcates economic sanctions that are acceptable under international law from those that are not).

87. On the salience of examining incidents in the identification of international law norms, see W. Michael Reisman, *International Incidents: Introduction to a New Genre in the Study of International Law*, 10 YALE J. INT'L L. 1, 3 (1984) ("The normative expectations that political analysts infer from events are the substance of much of contemporary international law.").

88. *See* Oliver Lissitzyn, Editorial Comment, *Some Legal Implications of the U-2 and RB-47 Incidents*, 56 AM. J. INT'L L. 135, 135 (1962) (describing the incident).

89. *See id.* at 136 (describing the incident).

90. *Department Statement, May 7*, DEP'T OF ST. BULL., Jan. 4, 1960, at 818; *Text of Soviet Note*, DEP'T OF ST. BULL., July 11, 1960, at 164.

91. *RB-47H Shot Down*, NATIONAL MUSEUM OF THE U.S. AIR FORCE (June 2, 2015), http://www.nationalmuseum.af.mil/Visit/MuseumExhibits/FactSheets/Display/tabid/509/Article/1

national airspace, and thereby the Soviet Union's territorial sovereignty, the latter, at least in the U.S. view, did not.

Four decades later, in 2001, U.S. military personnel aboard an unarmed EP-3 reconnaissance aircraft were detained after making a forced landing on a Chinese island following a mid-air collision with a Chinese fighter. China protested the nonconsensual landing, claiming, in part, that the American aircraft had "entered China's airspace without permission, [thereby] seriously violating China's territorial sovereignty."[92] The United States responded that the aircraft had been outside Chinese national airspace at the time of the collision and only entered it once in distress. It argued that while "military aircraft normally require permission to enter the territorial airspace of another nation," the wrongfulness of penetrating foreign airspace while in distress is precluded.[93] The dispute in the case was not over the existence of a rule prohibiting unconsented-to entry into another State's sovereign airspace, but rather the application of a circumstance precluding wrongfulness. Indeed, by relying on the notion of distress, it can only be concluded that the United States accepted that the action would, absent such a circumstance, have amounted to an internationally wrongful act.

The debate over counterterrorist drone strikes similarly have focused attention on respect for sovereignty and territorial integrity. Although drone operations implicate the prohibition on the use of force, States regularly characterize them as sovereignty violations. For instance, Pakistan has repeatedly taken the position that "drone strikes on its territory are counterproductive, contrary to international law, a violation of Pakistani sovereignty and territorial integrity, and should cease immediately."[94] Russian Foreign Minister Sergey Lavrov has echoed this position, stating, "It is not right to violate the sovereignty and integrity of any State. We fully support Pakistan's stance."[95] As explained below, the U.S. justification for the strikes likewise is framed in the narrative of sovereignty.

Analogous incidents have taken place at sea. In March 2007, fifteen British military personnel from the HMS Cornwall were searching a merchant dhow in the Persian Gulf[96] when they were captured and subsequently detained for nearly two weeks by Iranian Islamic Revolutionary

---

97621/rb-47h-shot-down.aspx [https://perma.cc/R9GS-D3K9]. On the distinction, see also Lissitzyn, *supra* note 88, 136–37.

92. Surveillance Activities and Emergency Landing by U.S. Aircraft on Hainan Island, People's Republic of China, 2001 DIGEST OF UNITED STATES PRACTICE IN INTERNATIONAL LAW, ch. 12, § A(6)(3) at 707.

93. *Id.* at 708.

94. Ben Emmerson (Special Rapporteur), Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, ¶ 54, U.N. Doc. A/68/389 (Sept. 18, 2013).

95. Omer Farooq Khanl, *Russia Backs Pakistan Fury on US Drones*, TIMES INDIA (Oct. 5, 2012), http://timesofindia.indiatimes.com/world/pakistan/Russia-backs-Pakistan-fury-on-US-drones/articleshow/16678916.cms [https://perma.cc/D9VF-V36U].

96. The operation was conducted in accordance with S.C. Res. 1723 (Nov. 28, 2006).

Guard forces.[97] Each side claimed the other had acted unlawfully based on the location of the incident; the United Kingdom stated that its forces were in Iraqi territorial waters, whereas Iran asserted that they were operating in Iranian waters. An Iranian Foreign Ministry spokesman, for example, argued that the British forces were "violating the sovereign boundaries" of Iran at the time of their seizure.[98] An investigation by the British Ministry of Defence concluded that a factor contributing to the incident was "[t]he absence of an internationally agreed delineation of Territorial Waters (TTW) and [Northern Arabian Gulf] water-space coordination measures between Iraq, Iran and Coalition Authorities."[99] The dispute was conducted in the vernacular of the violation of territorial sovereignty.

Nine years after the British–Iranian incident, the Iranian Islamic Revolutionary Guard Corps captured two U.S. Navy riverine craft with military personnel aboard after they mistakenly penetrated Iranian territorial waters. The Revolutionary Guards labeled the incident an "illegal entry into the Islamic Republic of Iran's waters."[100] Following negotiations, the ten individuals were released and the boats returned. Far from criticizing Iran for its actions in seizing the crew, Secretary of State John Kerry thanked them for their cooperation.[101] The United States understood the boats had violated Iranian sovereignty, albeit mistakenly.

Standing maritime territorial disputes regularly generate breach of territorial sovereignty claims. Most well known are those over South China Sea maritime boundaries, which are disputed by multiple countries in the region. The U.S. Navy conducts "Freedom of Navigation" (FON) operations in areas where it believes China has made excessive maritime claims, and China typically shadows the warships and warns them out of its purported territory.[102] Such disputes even arise among close allies. For instance, in a

---

97. *Seized Sailors 'Taken to Tehran'*, BBC NEWS (Mar. 24, 2007), http://news.bbc.co.uk/2/hi/uk_news/6489493.stm [https://perma.cc/E9XF-X4KU].

98. *Iran Claims U.K. Troops Admit to Illegal Entry*, NBC NEWS (Mar. 24, 2007), http://www.nbcnews.com/id/17769296/ns/world_news-mideast_n_africa/t/iran-claims-uk-troops-admit-illegal-entry/ [https://perma.cc/2BC9-DB9B].

99. MINISTRY OF DEFENCE, UK BOARDING OPERATIONS BY CTF 158 IN THE NORTHERN ARABIAN GULF (NAG), 2007, CJO/D/LM (20/07) (UK).

100. *Iran Frees Captured US Marines*, FARS NEWS AGENCY (Jan. 13, 2016), http://en.farsnews.com/newstext.aspx?nn=13941023000875 [https://perma.cc/C74A-ZNPP].

101. David E. Sanger et al., *Iran's Swift Release of U.S. Sailors Hailed as a Sign of Warmer Relations*, N.Y. TIMES (Jan. 13, 2016), https://www.nytimes.com/2016/01/14/world/middleeast/iran-navy-crew-release.html?_r=0 [https://perma.cc/8CCQ-REJY].

102. Kristina Daugirdas & Julian D. Mortenson, *United States Conducts Naval Operation Within Twelve Nautical Miles of Spratly Islands in the South China Sea, Prompting Protests from China*, 110 AM. J. INT'L L. 120, 120 (2016). For background and information on the Freedom of Navigation Program, see the Department of Defense's fact sheet, U.S. DEP'T OF DEF., FREEDOM OF NAVIGATION PROGRAM FACT SHEET (2015), http://policy.defense.gov/Portals/11/Documents/gsa/cwmd/DoD%20FON%20Program%20—%20Fact%20Sheet%20(March%202015).pdf [https://perma.cc/LT9Y-FFAE].

well-known 1985 incident, a Coast Guard icebreaker navigated through the Northwest Passage, which the United States claims is an international strait, without seeking Canadian permission.[103] In response, Canada "granted permission" (despite the lack of a request to that effect) for the voyage and, although the two countries agreed to the presence of Canadian observers onboard, the United States still disputed the Canadian claim of sovereignty over the waters.[104]

On land, the abduction of Adolph Eichmann is a classic case regarding territorial sovereignty. Eichmann had headed the Gestapo's Section for Jewish Affairs and was responsible for implementation of the Final Solution.[105] Following the war, he fled to Argentina.[106] In May 1960, the Israeli Mossad abducted Eichmann from Argentina and brought him to Israel for trial in the District Court of Jerusalem.[107]

Following the incident, but before trial, Argentina elevated the issue to the U.N. Security Council. In a letter to the Security Council, it submitted that "[t]he illicit and clandestine transfer of Eichmann from Argentine territory constitutes a flagrant violation of the Argentine State's right of sovereignty."[108] After considering the matter, the Council adopted Resolution 138, in which it observed that the "violation of the sovereignty of a Member State is incompatible with the Charter of the United Nations," and requested that the Israeli government make appropriate reparation for its actions.[109] Israel and Argentina subsequently issued a joint communiqué stating that they viewed as settled "the incident which was caused through the action of citizens of Israel that has violated the basic rights of the State of Argentina."[110]

In dealing with the question of whether a covert abduction operation in another country without that country's consent negated its jurisdiction, the

---

103. Michael Byers, *The Need to Defend Our New Northwest Passage*, TYEE (Jan. 30, 2006), https://thetyee.ca/Views/2006/01/30/DefendNorthwestPassage/ [https://perma.cc/VFD6-98GW].

104. *Id.*

105. *Adolf Eichmann*, U.S. HOLOCAUST MEMORIAL MUSEUM: HOLOCAUST ENCYCLOPEDIA, https://www.ushmm.org/wlc/en/article.php?ModuleId=10007412 [https://perma.cc/8P6J-SF65].

106. *Id.*

107. *Id.*

108. Letter from Mario Amadeo, Representative of Arg., to the U.N. Sec. Council, U.N. Doc. S/4336 (June 15, 1960).

109. S.C. Res. 138, pmbl., ¶ 2 (June 23, 1960). The explicit reference to a "violation of the sovereignty of a Member State" appears in the resolution's preamble, whereas the operative part cites "acts . . . which affect the sovereignty of a Member State." *Id.* pmbl., ¶ 1. This should not be interpreted as if the Security Council may not necessarily have regarded Israel's action as unlawful. On the contrary, because the Security Council directed Israel to provide reparation "in accordance with . . . the rules of international law," it must have concluded that a violation of international law had occurred; otherwise, no obligation to provide reparation would have materialized. *Id.* ¶ 2.

110. CrimC (Jer) 40/61 Att'y-Gen. of the Gov't of Isr. v. Eichmann, PM 5722 ¶ 50 (1962) (Isr.) (quoting the Joint Communiqué of Israel and Argentina, *reprinted in* Att'y-Gen. of the Gov't of Isr. v. Eichmann, 36 I.L.R. 59 (Isr., Dist. Ct. of Jerusalem 1961)).

District Court did not question the position that disrespect for territorial sovereignty can constitute a violation of international law. Clearly operating from the premise that such activities can do so, it concluded:

> [N]ow that the Governments of Argentina and Israel have issued their joint communique . . . to the effect that both governments have decided to view as liquidated the "incident" whereby the sovereignty of Argentina was violated, the Accused in this case can certainly retain no right to base himself on the "violated sovereignty" of the State of Argentina. The indictment in this case was presented after Argentina had forgiven Israel for that violation of her sovereignty, so that there no longer subsisted any violation of international law. In these circumstances, the Accused cannot presume to be speaking on behalf of Argentina and cannot claim rights which that sovereign state has waived.[111]

That an extraterritorial exercise of enforcement jurisdiction amounts to a violation of sovereignty of the State in which it occurs is now well settled in international law.[112]

An interesting incident concerning territorial sovereignty over both national airspace and land occurred in 1978, when a Soviet spacecraft with a nuclear reactor onboard, Cosmos 954, reentered the earth's atmosphere into Canadian airspace.[113] During reentry, the spacecraft disintegrated and debris was scattered across a wide swath of Canada. Canada claimed for compensation, both on the basis of the Convention on International Liability

---

111. *Id.* ¶ 44.

112. "A state's law enforcement officers may exercise their functions in the territory of another state only with the consent of the other state, given by duly authorized officials of that state." RESTATEMENT (THIRD) OF FOREIGN RELATIONS § 432(2) (AM. LAW INST. 1986). Professor Louis Henkin suggested that "[w]hen done without consent of the foreign government, abducting a person from a foreign country is a gross violation of international law and gross disrespect for a norm high in the opinion of mankind. It is a blatant violation of the territorial integrity of another state . . . ." Louis Henkin, *A Decent Respect to the Opinions of Mankind*, 25 JOHN MARSHALL L. REV. 215, 231 (1992). The fact that a State's unauthorized exercise of extraterritorial-enforcement jurisdiction amounts to a violation of the other State's sovereignty is also acknowledged in *Tallinn Manual 2.0*. TALLINN MANUAL 2.0, *supra* note 12, at 19, 67 (noting "[t]he Experts agreed that a violation of sovereignty occurs whenever one State physically crosses into the territory or national airspace of another State without either its consent or another justification in international law . . . " and stating "the exercise of enforcement jurisdiction on another State's territory constitutes a violation of that State's sovereignty . . . except when international law provides a specific allocation of authority to exercise enforcement jurisdiction extraterritorially or when the State in which it is to be exercised consents"). Similarly, the U.N. High Commissioner for Human Rights has accepted that an extraterritorial exercise of jurisdiction may violate another State's sovereignty. Rep. of the Office of U.N. High Comm'r for Hum. Rts. on the Right to Privacy in the Digital Age, ¶ 34, U.N. Doc. A/HRC/27/37 (June 30, 2014).

113. *See* Settlement of Claim Between Canada and the Union of Soviet Socialist Republics for Damage Caused by "Cosmos 954," Canada–U.S.S.R., Apr. 2, 1981 [hereinafter Settlement of Claim].

for Damage Caused by Space Objects[114] and "general principles of international law."[115] The dispute was settled in 1981 by means of a protocol between Canada and the Soviet Union.[116] Of particular relevance to the issue of territorial sovereignty was the approach taken by Canada in its Statement of Claim:

> The intrusion of the Cosmos 954 satellite into Canada's air space and the deposit on Canadian territory of hazardous radioactive debris from the satellite constitutes a violation of Canada's sovereignty. This violation is established by the mere fact of the trespass of the satellite, the harmful consequences of this intrusion, being the damage caused to Canada by the presence of hazardous radioactive debris and the interference with the sovereign right of Canada to determine the acts that will be performed on its territory. International precedents recognize that a violation of sovereignty gives rise to an obligation to pay compensation.[117]

Regarding *opinio juris*, senior government officials in many nations have referred for decades to the violation of sovereignty in a fashion that qualifies as such. Soviet Prime Minister Khrushchev, for example, in pointing to the notion of coexistence, stated in 1959 that:

> Apart from the commitment to nonaggression, [coexistence] also presupposes an obligation on the part of all states to desist from violating each other's territorial integrity and sovereignty in any form and under any pretext whatsoever. The principle of peaceful coexistence signifies a renunciation of interference in the internal affairs of other countries with the object of altering their system of government or mode of life or for any other motives.[118]

Note that Khrushchev not only confirmed Soviet acceptance of a rule prohibiting violation of territorial sovereignty, but also treated it separately from interference in internal affairs (coercive intervention).

Similarly, U.S. government representatives regularly offer expressions of *opinio juris* that operate from the premise of territorial sovereignty's inviolability. To illustrate, numerous statements, including ones issued with other States, were made on this basis during, and in the aftermath of, the conflict between Georgia and Russia in 2009. Following the ceasefire, for example, the State Department's spokesperson noted that Russia's plans to build up its military presence in the Georgian regions of Abkhazia and South

---

114. Convention on International Liability for Damage Caused by Space Objects art. II, Mar. 29, 1972, 24 U.S.T. 2389, 961 U.N.T.S. 187.

115. Settlement of Claim, *supra* note 113, ¶ 14.

116. Protocol in Respect of the Claim for Damages Caused by the Satellite "Cosmos 954," Canada–U.S.S.R, Apr. 2, 1981. 1470 U.N.T.S. 269.

117. Settlement of Claim, *supra* note 113, ¶ 21.

118. Nikita S. Khrushchev, *On Peaceful Coexistence*, 38 FOREIGN AFFAIRS 1, 3 (1959).

Ossetia would not only breach the ceasefire agreement but also violate Georgia's sovereignty and territorial integrity.[119]

More recently, Russian activities with respect to the Ukraine conflict, including Russia's belligerent occupation of the Crimean peninsula since 2014, have consistently been portrayed as violations of sovereignty. President Obama characterized Russian actions as such when discussing the matter with President Putin in March 2014.[120] The same month, the United States delivered a statement at the U.N. Human Rights Council on behalf of forty-two nations expressing concern over Russia's "ongoing violation of Ukraine's sovereignty and territorial integrity";[121] the G-7 did likewise.[122] President Obama then stated that Russia "flagrantly violated the sovereignty and territory of an independent European nation, Ukraine" during his "Address to the People of Europe" in April,[123] a claim he repeated at the NATO Warsaw Summit the same year.[124]

Many relevant statements have been made with respect to counterterrorist operations. In a speech at National Defense University in 2013, President Obama noted that "our actions are bound by consultations with partners, and respect for state sovereignty."[125] Other members of his administration repeatedly made the same point.[126] Attorney General Eric

---

119. Russia/Georgia, 2009 DIGEST OF UNITED STATES PRACTICE IN INTERNATIONAL LAW, ch. 18, §A(1)(b)(2) at 689; *see also* Ian Kelly, Statement on the 24th Round of the Geneva Discussions on the Conflict in Georgia (July 4, 2013), https://osce.usmission.gov/jul_4_13_georgia/ [https://perma.cc/6R3Y-JGXE].

120. Megan Slack, *Responding to the Situation in Ukraine*, WHITE HOUSE (Mar. 20, 2014), https://obamawhitehouse.archives.gov/blog/2014/02/20/responding-situation-ukraine [https://perma.cc/V7US-C4HS].

121. *Joint Statement by 42 States at the Human Rights Council on the Situation in Ukraine*, THE UNITED STATES MISSION TO THE UNITED NATIONS AND OTHER INTERNATIONAL ORGANIZATIONS IN GENEVA (Mar. 26, 2014), https://geneva.usmission.gov/2014/03/26/joint-statement-by-42-states-at-the-human-rights-council-on-the-situation-in-ukraine/ [https://perma.cc/Q2UC-CBKA].

122. *G-7 Leaders Statement*, WHITE HOUSE (Mar. 2, 2014), https://obamawhitehouse.archives.gov/the-press-office/2014/03/02/g-7-leaders-statement [https://perma.cc/5KGS-FJXR].

123. *Remarks by President Obama in Address to the People of Europe*, WHITE HOUSE (Apr. 25, 2016), https://obamawhitehouse.archives.gov/the-press-office/2016/04/25/remarks-president-obama-address-people-europe [https://perma.cc/R3N4-B2E2].

124. *Press Conference by President Obama after NATO Summit*, WHITE HOUSE (July 9, 2016), https://obamawhitehouse.archives.gov/the-press-office/2016/07/09/press-conference-president-obama-after-nato-summit [https://perma.cc/ZZ38-5NTP].

125. *Remarks by the President at the National Defense University*, WHITE HOUSE (May 23, 2013), https://obamawhitehouse.archives.gov/the-press-office/2013/05/23/remarks-president-national-defense-university [https://perma.cc/A26W-6NTV].

126. John O. Brennan, *Remarks of John O. Brennan, "Strengthening our Security by Adhering to our Values and Laws"*, WHITE HOUSE (Sept. 16, 2011), https://obamawhitehouse.archives.gov/the-press-office/2011/09/16/remarks-john-o-brennan-strengthening-our-security-adhering-our-values-an [https://perma.cc/X3TT-Z2JF]; Jeh Johnson, *Jeh Johnson's Speech on "National Security Law, Lawyers and Lawyering in the Obama Administration"*, COUNCIL ON FOREIGN REL. (Feb. 22, 2012), https://www.cfr.org/national-

Holder, speaking at Northwestern University School of Law, earlier had confirmed that "[i]nternational legal principles, including respect for another nation's sovereignty, constrain our ability to act unilaterally."[127] His comments were especially salient, for the Justice Department renders the final decision on questions of law for the Executive Branch.[128] The thread running through all of the statements has been recognition of an affirmative legal duty to respect the territorial sovereignty of other States in the conduct of U.S. counterterrorist operations; as a legal obligation, the duty represents a substantive rule, not simply the articulation of a broad normative principle or a restatement of the prohibitions of the use of force or coercive intervention.

Increasingly, senior U.S. government officials have acknowledged this duty with respect to activities in cyberspace. State Department Legal Adviser Harold Koh offered the first major statement on the matter in 2012 at an interagency legal conference convened at U.S. Cyber Command.[129] In the speech, he addressed the issue of sovereignty head on.

> States conducting activities in cyberspace must take into account the sovereignty of other States, including outside the context of armed conflict. The physical infrastructure that supports the internet and cyber activities is generally located in sovereign territory and subject to the jurisdiction of the territorial State. Because of the interconnected, interoperable nature of cyberspace, operations targeting networked information infrastructures in one country may create effects in another country. Whenever a State contemplates conducting activities in cyberspace, the sovereignty of other States needs to be considered.[130]

The position was clear. Remote cyber operations that cause effects in other States implicate, inter alia, the territorial sovereignty of those States. Koh spoke to the fact that it is incumbent on the State planning a remote cyber operation to consider whether the effects generated abroad breach the obligation to respect other States' territorial sovereignty; while he did not

---

security-and-defense/jeh-johnsons-speech-national-security-law-lawyers-lawyering-obama-administration/p27448 [https://perma.cc/6HHS-LZEE].

127. *Attorney General Eric Holder Speaks at Northwestern University School of Law*, U.S. DEP'T OF JUSTICE (Mar. 5, 2012), https://www.justice.gov/opa/speech/attorney-general-eric-holder-speaks-northwestern-university-school-law [https://perma.cc/KFH8-4N44].

128. 28 U.S.C. §§ 511–13 (1966). Consider this statute in light of 28 C.F.R. § 0.25 (2017).

129. Harold Koh, Legal Adviser of the U.S. State Dep't, Remarks at the U.S. Cyber Command Inter-Agency Legal Conference (Sept. 18, 2012) (transcript available at Chris Borgen, *Harold Koh on International Law in Cyberspace*, OPINIO JURIS (Sept. 19, 2012), http://opiniojuris.org/2012/09/19/harold-koh-on-international-law-in-cyberspace/ [https://perma.cc/MJS5-XJVA]).

130. *Id.* On the speech in relation to *Tallinn Manual 1.0*, see Michael N. Schmitt, *International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed*, 54 HARV. INT'L L.J. ONLINE 13 (2012).

answer the question of when cyber operations violate sovereignty, he clearly accepted that in certain circumstances they do.

In a 2016 address at Berkeley Law School, Koh's successor, Brian Egan, explicitly confirmed this point.

> The very design of the Internet may lead to some encroachment on other sovereign jurisdictions. Precisely when a nonconsensual cyber operation violates the sovereignty of another State is a question lawyers within the U.S. government continue to study carefully, and it is one that ultimately will be resolved through the practice and *opinio juris* of States.[131]

There was no suggestion that either of the former State Department Legal Advisers believed that sovereignty-related internationally wrongful acts in cyberspace were limited to uses of force or coercive intervention. On the contrary, both acknowledged that the principle of sovereignty applies in the cyber context and, by virtue of its legally binding nature, has operational significance.

This position tracks that contained in the 2014 U.S. submission to the U.N. Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (GGE). Stressing the application of sovereignty rules to the extraterritorial causation of effects, it noted,

> Most cyber activities undertaken by States and other actors fall below the threshold of the use of force and outside of the context of armed conflict. Such activities, however, do not take place in a legal vacuum. Instead, they are governed by, inter alia, international legal principles that pertain to State sovereignty, human rights, and State responsibility.
>
> . . . .
>
> State sovereignty, among other long-standing international legal principles, must be taken into account in the conduct of activities in cyberspace, including outside of the context of armed conflict. Because of the interconnected, interoperable nature of cyberspace, operations targeting networked information infrastructures in one country can have effects in many countries around the world. Whenever a State contemplates conducting activities in cyberspace, the sovereignty of other States needs to be considered.[132]

---

131. Brian J. Egan, Legal Adviser, U.S. Dep't of State, Remarks at Berkeley Law School on International Law and Stability in Cyberspace (Nov. 10, 2016), https://www.law.berkeley.edu/wp-content/uploads/2016/12/egan-talk-transcript-111016.pdf [https://perma.cc/B6TH-232L].

132. Applicability of International Law to Conflicts in Cyberspace, 2014 DIGEST OF UNITED STATES PRACTICE IN INTERNATIONAL LAW, ch. 18, § A(3)(b), at 737. Interestingly, the Department of Defense's own Law of War Manual emphasizes the obligation in an armed conflict to respect the sovereignty of other States during cyber operations because "cyber operations targeting networked information infrastructures in one State may create effects in another State that is not a party to the

Other States also apply a substantive, vice foundational, rule of territorial inviolability to cyber activities, distinguishing it from separate relevant primary rules of international law. For instance, indicative of the Netherlands government's views were the opening comments of the Foreign Minister Bert Koenders at the 2017 European launch of *Tallinn Manual 2.0*.[133] In his speech, he noted that "we mustn't be naive. Cyber operations against institutions, political parties and individuals underline why we need the international legal principles of sovereignty and nonintervention in the affairs of other states."[134] In light of the hostile cyber operations he cited, the Minister can only have attributed operational consequence to the principle of sovereignty, which he distinguished from nonintervention. He went on to emphasize that "[t]he Tallinn Manual provides guidance on the application of long-established legal principles in the cyber domain: sovereignty, nonintervention, due diligence, and state responsibility."[135] That guidance, as explained, attributes primary-rule significance to sovereignty, a point that could not have been lost on the Netherlands Ministry of Foreign Affairs.

C. Sovereignty in International Fora

Both the U.N. Security Council and the General Assembly have treated the violation of sovereignty as a primary rule. For example, the Security Council resolution cited above in the Eichmann case specifically referred to "violation of the sovereignty of a Member State."[136] But among resolutions by U.N. organs, the General Assembly's 1970 Declaration on Friendly

---

armed conflict." U.S. DEP'T OF DEF., OFFICE OF GEN. COUNSEL, LAW OF WAR MANUAL 1019 (2016). Although framed in the context of neutrality, such an operation in an international armed conflict could breach the State's obligations with respect to both territorial sovereignty and neutrality. During a noninternational armed conflict, only the former would be breached, as the law of neutrality applies only to international armed conflicts. On neutrality, see Convention Concerning the Rights and Duties of Neutral Powers and Persons in War on Land arts. 5, 10, 17, Oct. 18, 1907, 36 Stat. 2310 (discussing the nature of international neutrality) and Convention Concerning the Rights and Duties of Neutral Powers in Naval War arts. 1–12, Oct. 18, 1907, 36 Stat. 2415 (establishing protocols for neutrality at sea). In the cyber context, see TALLINN MANUAL 2.0, *supra* note 12, at 553 (explaining the relationship between neutrality and cyber warfare).

133. Bert Koenders, Foreign Minister, Neth., Remarks at The Hague Regarding Tallinn Manual 2.0 (Feb. 13, 2017) (on file with authors).

134. *Id.* See also the report by noted international law experts that was commissioned by the government of the Netherlands which found that "[i]nternational law is based on a strict prohibition of the use of force and a duty to respect the sovereignty and territorial inviolability of other states. These rights and duties are a two-way street . . . ." ADVISORY COUNCIL ON INT'L AFFAIRS AND THE ADVISORY COMM. ON ISSUES OF PUB. INT'L LAW, No. 77 AIV/No. 22, CAVV, CYBER WARFARE 22 (2011).

135. Koenders, *supra* note 133.

136. S.C. Res. 138, *supra* note 109, pmbl.

Relations is perhaps the most significant general pronouncement of law bearing on the existence of such a rule.[137]

The resolution's text is especially noteworthy because it represents an unusual consensus during the divisive Cold War. In the Declaration, the General Assembly reaffirms "the basic importance of sovereign equality and [stresses] that the purposes of the United Nations can be implemented only if States enjoy sovereign equality and comply fully with the requirements of this principle in their international relations."[138] This carefully negotiated verbiage implies that there are certain State actions that are not in compliance with—that is, violate—the principle of sovereign equality. This can only be so if sovereignty is more than an underlying principle; it must have operative effect.

Sovereign equality is one of seven principles highlighted by the Declaration. As to the principle, the resolution observes: "In particular, sovereign equality includes the following elements: . . . (d) [t]he territorial integrity and political independence of the State are inviolable . . . ."[139] It is telling that the reference to territorial inviolability appears with regard to a principle, sovereign equality, that is set out separately from the principle requiring States to refrain from the threat or use of force against the territorial integrity or political independence of other States.[140] This being so, it can only be understood as applicable in its own right.

Treaty law sheds further light on the existence of a rule prohibiting violations of territorial sovereignty. The U.N. Convention Against Transnational Organized Crime, for example, provides,

> States Parties shall carry out their obligations under this Convention in a manner consistent with the principles of sovereign equality and territorial integrity of States and that of nonintervention in the domestic affairs of other States.
>
> . . . Nothing in this Convention entitles a State Party to undertake in the territory of another State the exercise of jurisdiction and performance of functions that are reserved exclusively for the authorities of that other State by its domestic law.[141]

Note how the first subparagraph distinguishes an act implicating sovereign equality and territorial integrity from one involving prohibited intervention, while the second deals with functions that are reserved to

---

137. G.A. Res. 2625 (XXV), Declaration on Principles of International Law Concerning Friendly Relations and Co-operation Among States in Accordance with the Charter of the United Nations (Oct. 24, 1970).

138. *Id.* pmbl.

139. *Id.* (under preamble section titled "The principle of sovereign equality of States").

140. *Id.* (under preamble section titled "The principle of equal rights and self-determination of peoples").

141. G.A. Res. 55/25, annex, U.N. Convention Against Transnational Organized Crime, art. 4 (Jan. 8, 2001).

another State, which, as explained above, is an additional basis for finding that an act violates sovereignty.

Other treaties likewise acknowledge the inviolability of territory. For instance, the Rio Treaty refers to "the inviolability or the integrity of the territory or the sovereignty or political independence of any American State."[142] The Charter of the Organization of American States provides that "[t]he territory of a State is inviolable."[143] It also sets forth a collective security scheme that applies "[i]f the inviolability or the integrity of the territory or the sovereignty or political independence of any American State should be affected by . . . any . . . fact or situation that might endanger the peace of America."[144]

Statements on sovereignty in the context of cyber operations have also begun to appear in international fora. In its 2013 report, the U.N. GGE, composed of representatives from fifteen States, stated 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."[145] Note how the GGE differentiates State sovereignty from the norms and principles that derive from sovereignty, thereby indicating a distinction between them. Also significant is the GGE's treatment of the applicability of sovereignty to cyber conduct in a way that distinguishes it from the mere exercise of jurisdiction over cyber activities.

The GGE's 2015 report expanded on this distinction:

> In their use of ICTs, States must observe, among other principles of international law, State sovereignty, sovereign equality, the settlement of disputes by peaceful means and nonintervention in the internal affairs of other States. Existing obligations under international law are applicable to State use of ICTs.[146]

In other words, the GGE singled out the principle of State sovereignty, differentiating it from that of nonintervention. Moreover, the GGE did so in a paragraph that discusses the law that regulates State cyber operations, thereby accepting that the principle of sovereignty limits the "use" of cyber technologies vis-à-vis other States as a matter of international law.

Finally, in 2016, the heads of State of the Shanghai Cooperation Organization issued a joint declaration in which they "call[ed] on the international community to develop a peaceful, secure, fair and open

142. Inter-American Treaty of Reciprocal Assistance (Rio Treaty) art. 6, Sept. 2, 1947, 62 Stat. 1681, 21 U.N.T.S. 77.

143. Charter of the Organization of American States art. 17, Apr. 30, 1948, 2 U.S.T. 2394, 119 U.N.T.S. 3.

144. *Id.* art. 25.

145. U.N. GGE 2013 Report, *supra* note 3, ¶ 20.

146. U.N. GGE 2015 Report, *supra* note 3, ¶ 28(b).

information space based on the principles of cooperation and respect for national sovereignty and noninterference in the internal affairs of other countries."[147] It is clear that the obligation to respect the sovereignty of other States enjoys wide recognition globally, including in the cyber context.

IV. Concluding Thoughts

Corn and Taylor worry that a rule requiring respect for territorial sovereignty would impede important operations necessary to national security. They warn,

> If the view were adopted that sovereignty is a rule violated by any action illegal under the domestic law of a state, states seeking to disrupt distributed terrorist cyber infrastructure would be under an obligation to either seek Security Council authorization or the consent of the state in whose territory the infrastructure resides. The nature of cyber operations and capabilities often require high degrees of operational security and the flexibility to act with speed and agility. Operating through a consent model could in important cases surrender operational initiative to the terrorist adversary or render response options unworkable.[148]

Their concern is misplaced, for they treat the rule prohibiting violation of territorial sovereignty as absolute. This badly misstates the view of those supporting its validity. The rule's proponents are clear that it does not apply to every remotely conducted cyber operation into another State's territory. Indeed, they are divided over those operations that do breach inviolability.[149] The assertion that the rule on sovereignty somehow would leave a State defenseless in the face of serious threats to national security is also counter-normative. International law provides a robust toolbox for a State wishing to respond to hostile cyber operations that includes retorsion,[150] countermeasures,[151] actions based on the plea of necessity,[152] and self-defense.[153]

Moreover, the consequences of the absence of such a rule for States that are the target of hostile cyber operations would be unacceptable. Although

---

147. *The Tashkent Declaration of the Fifteenth Anniversary of the Shanghai Cooperation Organization*, EMBASSY OF THE REPUBLIC OF UZBEKISTAN IN THE REPUBLIC OF LATVIA (June 28, 2016), http://uzbekistan.lv/en/the-tashkent-declaration-of-the-fifteenth-anniversary-of-the-shanghai-cooperation-organization/ [https://perma.cc/EC6V-QK6L].

148. Corn & Taylor, *supra* note 16.

149. *See* TALLINN MANUAL 2.0, *supra* note 12, at 19–21, 23.

150. Acts that, albeit unfriendly, are lawful, such as economic sanctions. *Id.* at 112.

151. Articles on State Responsibility, *supra* note 11, art. 22; TALLINN MANUAL 2.0, *supra* note 12, at 111 (Rule 20).

152. Articles on State Responsibility, *supra* note 11, art. 25; TALLINN MANUAL 2.0, *supra* note 12, at 135 (Rule 26).

153. U.N. Charter art. 51; TALLINN MANUAL 2.0, *supra* note 12, at 339 (Rule 71).

the precise threshold at which a cyber operation constitutes a use of force is unsettled in international law, it is undisputed that an offending operation must reach a high degree of severity. By the Corn and Taylor approach, operations falling below that threshold would be governed solely by the prohibition on coercive intervention. Yet a cyber operation that either does not affect a State's *domaine réservé* or that is not coercive would not be encompassed in the prohibition. As an example, consider a State's disruptive cyber operations directed against commercial cyber infrastructure in another State intended to give the former's own companies a competitive advantage. The operations would lie beyond the prohibition because such activities are generally not considered to fall within the *domaine réservé*. Also problematic is the fact that cyber operations that are merely malicious or vindictive lack the requisite element of coercion.

In law as in life, what one sees depends on where one stands. Corn and Taylor take the perspective of those charged with conducting cyber operations into other States to defend the United States or otherwise advance its national interests. Thus, it is unsurprising that, given the ease by which cyber operations cross borders and their increasing frequency and severity, they do not want the hands of the Department of Defense tied.

But one must wonder whether government departments charged with the conduct of diplomacy or fashioning policy responses to hostile cyber operations will be amenable to forgoing the option of labeling other States' hostile cyber operations as unlawful unless they cross the coercive-intervention or use-of-force thresholds, especially in light of the fact that the vast majority of the operations do not. Additionally, bringing down the normative firewall in the manner they propose would bar the taking of countermeasures in response to many hostile cyber operations because the operations would not qualify as internationally wrongful acts.[154]

States facing cyber threats, but lacking the cyber wherewithal of the United States, are likewise unlikely to countenance a legal regime that opens the gates wide to hostile cyber operations. It would leave them legally defenseless in the face of most such operations, and factually dependent on the United States or other cyber powers for assistance in responding to them. It is worth recalling that States enjoy sovereign equality; they all get a vote in the development and subsequent authoritative interpretation of international law. That the international community will accept the

154. Of course, by the Corn and Taylor approach, qualifying a cyber response as a countermeasure may not be necessary because under the scheme many of the responses themselves would not breach an obligation owed to the other State. Yet, because responses need not be in-kind to qualify as lawful countermeasures, their approach would also remove the option of engaging in noncyber countermeasures. TALLINN MANUAL 2.0, *supra* note 12, at 128. The nonavailability of countermeasures might be especially problematic from a policy perspective as the United States continues to search for effective means by which to deter other States' hostile cyber operations directed against it.

possibility of a cyber "wild west" below the intervention threshold is highly unlikely.

As has been demonstrated, Corn's and Taylor's arguments fly in the face of long-standing State practice, *opinio juris*, and judicial decisions as to the application of the primary rule of sovereignty that safeguards territorial integrity and inviolability. Indeed, they have cleverly attempted to shift the burden of persuasion in this regard. However, the evidence of the rule is so dense that those asserting its nonapplicability to cyber operations manifesting on the territory of another State must, as a matter of law, bear the burden of establishing why it does not apply to cyber operations. This they have failed to do. Instead, policy arguments and analysis are offered in the attempt to rebut a well-established legal notion.

Ultimately, Corn and Taylor conclude,

> [W]hether and precisely when non-consensual cyber operations below the threshold of a prohibited intervention violate international law is a question that must be resolved through the practice and *opinio juris* of states, developed over time and in response to the need of states effectively to defend themselves and provide security for their citizens.[155]

They are correct, but off course. Practice and *opinio juris*—and perhaps treaty law—will not determine whether territorial sovereignty is inviolable; it clearly is. Rather, practice and *opinio juris* will inform the contours of the rule as applied in the cyber context. Over time, it may even contribute to the emergence of *lex specialis* rules that provide for exceptions to the *lex generalis* rule protecting territorial integrity and inviolability. But for the present, such possibilities amount to nothing more than *lex ferenda*.

155. Corn & Taylor, *supra* note 16.

* * *

* * *

* * *


TEXAS
TLR
LAW REVIEW