Bibliography

International Organizations

1. UN

Declaration of Legal Principles Governing the Activities of States in the Exploration and Use of Outer Space, UNGA Res. 1962 (XVIII), U.N. Doc. A/RES/1962(XVIII) (13 Dec. 1963).

UNGA Res. 2625 (XXV), 24 Oct. 1970, Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations.

UNGA Res. 3314 (XXIX) on the Definition of Aggression (1974).

UN General Assembly Resolution on the Guidelines for the Regulation of Computerized Personal Data Files, Doc. A/RES/45/95 (14 Dec. 1990).

International Law Commission, *Draft Articles on Responsibility of States for International Wrongful Acts*, *ILC Yearbook*, 2001, vol. II, Part Two.

International Law Commission, *Draft Articles on Diplomatic Protection*, UNGA Off. Records, Sixty-first Session, Supplement No. 10 (A/61/10).

UN Security Council Resolution 1566 (2004)

UN Security Council Resolution 1816 (2008)

UN Security Council Resolution 2249 (2015)

UN Secretary-General's report *In Larger Freedom: Toward Security, Development and Human Rights for All*, UNGA Doc. A/59/2005 (21 Mar. 2005).

Havana Declaration, UN Doc. S/2006/780, 29 Sept. 2006.

Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, 28 Dec. 2009, UN Doc. A/HRC/13/37.

UN Guiding Principles for Business and Human Rights (New York and Geneva: United Nations Publication HR/PUB/11/04, 2011).

International Law Commission, *Draft Articles on the Effects of Armed Conflicts on Treaties*, *ILC Yearbook*, 2011, vol. II, part Two.

Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 17 Apr. 2013, UN Doc. A/HRC/23/40.

Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, UN Doc. A/HRC/17/27 (16 May 2011).

Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Doc. A/HRC/29/32 (22 May 2015).

K. Kittichaisaree, *Public International Law of Cyberspace*, Law, Governance and Technology Series 32, DOI 10.1007/978-3-319-54657-5

Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, UN Doc. A/HRC/32/38 (11 May 2016).
GGEs, *On the Developments in the Field of Information and Telecommunications in the Context of International Security* (24 Jun. 2013).
UNGA Res. 68/167, "The right to privacy in the digital age", 18 Dec. 2013.
Report of the Office of the High Commissioner for Human Rights, "The Right to Privacy in the Digital Age", 30 Jun. 2014, UN Doc. A/HRC/27/37.
Final Report of the International Law Commission on the Obligation to extradite or prosecute (*aut dedere aut judicare*), *ILC Yearbook*, 2014, vol. II (Part Two).
"Consideration of effective measures to enhance the protection, security and safety of diplomatic and consular missions and representatives", UNGA Res. A/69/121 (18 Dec. 2014).
Summary of the Human Rights Council panel discussion on the right to privacy in the digital age (UNGA Doc. A/HRC/28/39 dated 19 Dec. 2014).
UN Human Rights Council's resolution on the Right to Privacy in the Digital Age, A/HRC/28/L.27 (24 Mar. 2015).
UN High Commissioner for Refugees (UNHCR), Policy on the Protection of Personal Data of Persons of Concern to the UNHCR (May 2015).
GGEs, 2nd Report, UNGA Doc. A/70/174 (22 Jul. 2015).
Report of the UN Secretary-General on Somalia, *UN Doc. S/2016/27* (8 Jan. 2016).

2. EU

EU Council Framework Decision 2002/475/JHA on Combating Terrorism 2002.
EU Council Framework Decision 2008/919/JHA on Combating Terrorism 2008.
The Conclusions of the European Council (24/25 Oct. 2013), EUCO 169/13, available at: http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/ec/139197.pdf.
European Commission, Action Plan to Strengthen the Fight against Terrorist Financing (12 Feb. 2016).

3. OAS

Resolution on Strengthening Hemispheric Cooperation to Prevent, Combat, and Eliminate Terrorism, adopted at the 23rd meeting of Consultation OEA of Ministers of Foreign Affairs, 21 Sept. 2001, Ser.F/II.23/RC.23/RES.1/01.
United Nations Special Rapporteur on the Protection and Promotion of the Right to Freedom of Opinion and Expression; Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, "Joint declaration on surveillance programs and their impact on freedom of expression", available at: http://www.oas.org/en/iachr/expression/showarticle.asp?artID=927&lID=1.
Draft Preliminary Principles and Recommendation on Data Protection (the Protection of Personal Data), Permanent Council of the Organization of American States, Committee on Juridical and Political Affairs, OEA/Ser. G CP/CAJP-2921/10, 19 Nov. 2010.
Comparative Study: Data Protection in the Americas, Permanent Council of the Organization of American States, Committee on Juridical and Political Affairs, OEA/Ser. G CP/CAJP-3063/12, 3 Apr. 2012.

4. African Union

ECOWAS' 2010 Supplementary Act on Personal Data Protection

5. APEC

2005 APEC Privacy Framework (Singapore: APEC Secretariat)

6. ASEAN

Human Rights Declaration of the Association of Southeast Asian Nations (ASEAN) dated 19 Nov. 2012

Literature

Nikolas Abel, "*United States vs. Mehanna*, the First Amendment, and Material Support in the War on Terror," *Boston Coll. L. Rev.* 54 (2013): 711.

Jeffrey F. Addicott, "The Emerging Threat of Cyberterrorism" in *Understanding Terrorism: Analysis of Sociological and Psychological Aspects*, eds. Suleyman Ozeren, Ismail Dincer Gunes, and Diab M. Al-Badayneh (Amsterdam: IOS Press, 2007), 259.

Kai Ambos, "International Criminal Responsibility in Cyberspace" in *Research Handbook on International Law and Cyberspace*, eds. Nicholas Tsagourias and Russell Buchan (Cheltenham: Edward Elgar, 2015), 118.

American Bar Association Rule of Law Initiative, *The ASEAN Human Rights Declaration: A Legal Analysis* (Washington, DC: American Bar Assoc., 2014).

Edward G Amoroso, *Cyber Attacks: Protecting National Infrastructure* (Burlington, MA: Butterworth-Heinemann, 2011).

Jason Andress, Steve Winterfeld and Lillian Ablon, *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*, 2nd ed. (Amsterdam: Elsevier, 2014).

Constantine Antonopoulos, "State Responsibility in Cyberspace," in *Research Handbook on International Law and Cyberspace*, eds. Nicholas Tsagourias and Russell Buchan (Cheltenham : Edward Elgar, 2015), 30.

Louise Arimatsu, "Classifying Cyber Warfare" in *Research Handbook on International Law and Cyberspace*, eds. Nicholas Tsagourias and Russell Buchan (Cheltenham: Edward Elgar, 2015), 326.

Helmut Philipp Aust, *Complicity and the Law of State Responsibility* (Cambridge: Cambridge University Press, 2011).

Greg Austin, "International Legal Norms in Cyberspace: Evolution of China's National Security Motivations," in *International Cyber Norms: Legal, Policy & Industry Perspectives*, eds. Ann-Maria Osula and Henry Rõigas (Tallinn: NATO CCD COE, 2016).

Gianmarco Baldini, Maarten Botterman, Ricardo Neisse, and Mariachiara Tallacchini, "Ethical Design in the Internet of Things", *Sci. Eng. Ethics* (2016). doi: 10.1007/s11948-016-9754-5.

Karine Bannelier-Christakis, "Cyber Diligence: A Low-Intensity Due Diligence Principle for Low-Intensity Cyber Operations?", *Baltic YBIL* 14 (2014): 23.

———. "Is the Principle of Distinction Still Relevant in Cyberwarfare?" in *Research Handbook on International Law and Cyberspace*, eds. Nicholas Tsagourias and Russell Buchan (Cheltenham: Edward Elgar, 2015), 343.

Daphne Barak-Erez and David Scharia, "Freedom of Speech, Support for Terrorism and the Challenge of Global Constitutional Law," *Harvard Nat. Security J.* 2 (2011): 1.

Matthias Bauer, Hosuk Lee-Makiyama, Erik van der Marel, and Bert Verschelde, *The Costs of Data Localisation: Friendly Fire on Economic Recovery* (Brussels: ECIPE Occasional Paper No. 3/2014).

Paul Bernal, *Internet Privacy Rights: Rights to Protect Autonomy* (Cambridge: Cambridge University Press, 2014).

Igor Bernik, *Cybercrime and Cyberwarfare* (London: ISTE and John Wiley & Sons, 2014).

Daniel Bethlehem, "Principles relevant to the Scope of a State's Right of Self-Defence against an Imminent or Actual Armed Attack by Non-State Actors," *Amer. JIL* 106 (2012): 776.

———. "Principles of Self-Defence—A Brief Response," *Amer. JIL* 107 (2013): 579.

F. Bignami, "European Versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data Mining," *B.C.L. Rev* 48 (2007): 609.

Jeffrey Thomas Biller, "Cyber-Terrorism: Finding a Common Starting Point", LL.M. thesis, George Washington University Law School, 2012.

P. Blume, "Data Protection and Privacy - Basic Concepts in a Changing World," *Scandinavian Stud. L.* 56 (2010): 151.

Derek Bowett, *Self-Defence in International Law* (Manchester: Manchester University Press, 1958).

Susan W. Brenner, *Cyberthreats and the Decline of the Nation-State* (London/New York: Routledge, 2014).

Ove Bring, "The Use of Force under the UN Charter: Modification and Reform through Practice of Consensus," in *International Law and Changing Perceptions of Security: Liber Amicorum Said Mahmoudi*, eds. J. Ebbesson, M. Jacobsson, M. Klamberg, D. Langlet and P. Wrange (Leiden/Boston: Brill Nijhoff, 2014), 1.

Ian Brownlie, *International Law and the Use of Force by States* (Oxford: Clarendon Press, 1963).

Roger Brownsword and Morag Goodwin, *Law and the Technologies of the Twenty-First Century: Text and Materials* (Cambridge: Cambridge University Press, 2012).

Steven Bucci, "Joining Cybercrime and Cyber Terrorism: *A Likely Scenario*" in *Cyber Challenges and National Security: Threats, Opportunities, and Power in a Virtual World*, ed. Derek S. Reveron (Washington, DC: Georgetown University Press, 2012), 65.

Russell Buchan, "The International Legal Regulation of State-Sponsored Cyber Espionage," in *International Cyber Norms: Legal, Policy & Industry Perspectives*, eds. Anna-Maria Osula and Henry Rõigas (Tallinn: NATO CCD COE, 2016), 65.

Cedric Burton, Laura De Boel, Christopher Kuner, Anna Pateraki, Sarah Cadiot, and Sára G. Hoffman, "The Final European Union General Data Protection Regulation", 15 *Privacy and Security Law Rep.* 15 (2016): 153.

Antoine Buyse, "Dangerous Expressions: The ECHR, Violence and Free Speech," *Int'l & Comp. L. Quarterly* 63 (2014): 491.

———. "Words of Violence: Relating Violent Conflict Escalation to the Boundaries of the Freedom of Expression," *Human Rights Quarterly* 36 (2014): 779.

Lee A. Bygrave, *Data Protection Law: Approaching Its Rationale, Logic and Limits* (The Hague: Kluwer, 2002).

———. *Data Privacy Law: An International Perspective* (Oxford: Oxford University Press, 2014).

Lee A. Bygrave and Jon Bing, eds., *Internet Governance: Infrastructure and Institutions* (Oxford: Oxford University Press, 2011).

Dennis Campbell and Chrysta Bán, eds., *Legal Issues in the Global Information Society* (Dobbs Ferry, NY: Oceana, 2005).

Elaine Campbell, "The New Age of Surveillance", *Harvard L. Bull.* (Spring 2016): 38.

Indira Carr, Jahid Bhuiyan, and Shawkat Alam, eds., *International Trade Law and WTO* (Annandale, NSW, Australia: Federation Press, 2012).

S. Casey-Maslen, ed., *The War Report 2012* (Oxford: Oxford University Press, 2013).

Antonio Cassese, *International Criminal Law* (Oxford: Oxford University Press), 1st ed. (2003); 2nd ed. (2008); 3rd ed. (2013).

Manuel Castells, *Networks of Outrage and Hope: Social Movements in the Internet Age*, 2nd ed. (Cambridge: Polity, 2015).

Ilias Chantzos and Shireen Alam, "Technological Integrity and the Role of Industry in Emerging Cyber Norms," *in International Cyber Norms: Legal, Policy & Industry Perspectives*, eds. Anna-Maria Osula and Henry Rõigas (Tallinn: NATO CCD COE, 2016), chap. 10.

Maura Conway and Clive Walker, "Countering terrorism via the internet" in *Routledge Handbook of Law and Terrorism*, eds. Genevieve Lennon and Clive Walker (London and New York: Routledge, 2015), 416.

Geoffrey S. Corn, "Triggering the law of Armed Conflict?" in *The War on Terror and the Laws of War: A Military Perspective*, 2nd ed., eds. Geoffrey S. Corn et al. (New York: Oxford University Press, 2015), 33.

Geoffrey S. Corn, James A. Schoettler, Jr., Dru Brenner-Beck, Victor M. Hansen, Richard B. "Dick" Jackson, Eric Talbot Jensen, and Michael W. Lewis, *The War on Terror and the Laws of War: A Military Perspective*, 2nd ed. (New York: Oxford University Press, 2015).

Emily Crawford, *Identifying the Enemy: Civilian Participation in Armed Conflict* (Oxford: Oxford University Press, 2015).

F.H. Cate, J.X. Dempsey, and I.S. Rubinstein, "Systematic government access to private-sector data," *International Data Privacy Law* 2 (2012): 195.

George Curtis, *The Law of Cybercrimes and Their Investigations* (Boca Raton, FL: CRC Press, 2012).

Christian Czosseck, "State Actors and their Proxies in Cyberspace" in *Peacetime Regime for State Activities in Cyberspace*, ed. Katharina Ziolkowski (Tallinn: NATO CCD COE, 2013), 1.

Shane Darcy, *Judges, Law and War: The Juridical Development of International Humanitarian Law* (Cambridge: Cambridge University Press, 2012).

Jennifer Daskal, "The Un-Territoriality of Data," *Yale LJ* 125 (2015): 326.

Paul K. Davis, "Deterrence, Influence, Cyber Attack, and Cyber War", *Int'l L. & Politics* 47 (2015): 327.

Boudewijn de Bruin and Luciano Floridi, "The Ethics of Cloud Computing", *Sci. Eng. Ethics* (2016). doi:10.1007/s11948-016-9759-0.

Chris C. Demchak, "Economic and Political Coercion and a Rising Cyber Westphalia," in *Peacetime Regime for State Activities in Cyberspace,* ed. Katharina Ziolkowski (Tallinn: NATO CCD COE, 2013), 595.

Laura DeNardis, *The Global War for Internet Governance* (New Haven: Yale University Press, 2014).

Dorothy E. Denning, "Rethinking the Cyber Domain and Deterrence", *Joint Force Quarterly* 77 (Apr. 2015): 8.

E. Denza, *Diplomatic Law: Commentary on the Vienna Convention on Diplomatic Relations* (Oxford: Clarendon Press, 1998).

Oliver Diggermann and Maria Nicole Cleis, "How the Right to Privacy Became a Human Right," *European Human Rights L. Rev.* 14 [2014]: 441.

Julian Ding, "Internet Regulation" in *Legal Issues in the Global Information Society*, eds. Dennis Campbell and Chrysta Bán (Dobbs Ferry, NY: Oceana, 2005), 306.

Heather Harrison Dinniss, *Cyber Warfare and the Laws of War* (Cambridge: Cambridge University Press, 2012).

Yoram Dinstein, "Computer Network Attacks and Self-Defense," in *Computer Network Attack and International Law*, eds. Michael N. Schmitt and Brian T. O'Donnell (New Port, Rhode Island: US Naval War College, 2002), 99.

———. *War, Aggression and Self-Defence*, 5th ed. (Cambridge: Cambridge University Press, 2011).

———. *The Conduct of Hostilities under the Law of International Armed Conflict*, 3rd ed. (Cambridge: Cambridge University Press, 2016).

Knut Dörmann, "Computer network attack and international humanitarian law" (paper presented at the Internet and State Security Forum, Trinity College, Cambridge, UK, 19 May 2001).

———. "Applicability of the Additional Protocols to Computer Network Attacks" (paper presented at the International Expert Conference on Computer Network Attacks & the Applicability of International Humanitarian Law, Stockholm, 17–19 Nov. 2004).

David M. Douglas, "Towards a just and fair Internet: applying Rawls' principles of justice to Internet regulation", *Ethics Inf. Technol.* 17 (2015): 57.

———. "Doxing: a conceptual analysis", *Ethics Inf. Technol.* 18 (2016): 199.

Michael Doyle, "A Global Constitution?: The Struggle over the UN Charter" (paper presented at the New York University Symposium, 22 Sept. 2010).

Paul Ducheine, "The Notion of Cyber Operations," in *Research Handbook on International Law and Cyberspace*, eds. Nicholas Tsagourias and Russell Buchan (Cheltenham : Edward Elgar, 2015), 211.

J. Ebbesson, M. Jacobsson, M. Klamberg, D. Langlet and P. Wrange, eds., *International Law and Changing Perceptions of Security: Liber Amicorum Said Mahmoudi* (Leiden/Boston: Brill Nijhoff, 2014).

Brian Egan, "International Law, Legal Diplomacy, and the Counter-ISIL Campaign" (paper presented at the Annual Meeting of the American Society of International Law, 30 Mar.-2 Apr. 2016).

Victoria Ekstedt, Tom Parkhouse, and Dave Clemente, "Commitments, Mechanism & Governance," in *National Cyber Security Framework Manual*, ed. Alexander Klimburg (Tallinn: NATO CCD COE Publication, 2012), 155.

M. Ena, "Securing Online Transaction: Crime Prevention Is the Key, "*Fordham Urban L.J.* 35 (2008): 147.

Astrid Epiney and Tobias Fasnacht, eds., *Le développement du droit européen en matière de protection des données et ses implications pour la Suisse* (Zurich: Schulthess, 2012).

European Court of Human Rights' Research Division, *National security and European case-law* (Strasbourg: Council of Europe/European Court of Human Rights, 2013).

Bardo Fassbender, *The United Nations Charter as the Constitution of the International Community* (Leiden/Boston: Martinus Nijhoff/Brill, 2009).

David P. Fidler, "Cyberspace and Human Rights" in *Research Handbook on International Law and Cyberspace*, eds. Nicholas Tsagourias and Russell Buchan (Cheltenham : Edward Elgar, 2015), 94.

Carlo Focarelli, "Self-Defence in Cyberspace" in *Research Handbook on International Law and Cyberspace*, eds. Nicholas Tsagourias and Russell Buchan (Cheltenham: Edward Elgar, 2015), 255.

Francesco Francioni and Natalino Ronzitti, eds., *War by Contract: Human Rights, Humanitarian Law, and Private Contractors* (Oxford: Oxford University Press, 2011).

Iginio Gagliardone and Nanjira Sambuli, "Cyber Security and Cyber Resilience in East Africa", *Global Commission on Internet Governance Paper Series No. 15* (Waterloo/Canada and London: Centre for International Governance Innovation & Chatham House: May 2015).

Giorgio Gaja, "General Principles of Law" in *Max Planck Encyclopedia of Public International Law* (Oxford: Oxford University Press, 2013).

Peter Galison and Martha Minow, "Our Privacy, Ourselves in the Age of Technological Intrusions," in *Human Rights in the 'War on Terror'*, ed. Richard Ashby Wilson (Cambridge: Cambridge University Press, 2005), 258.

Robin Geiß and 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*, ed. Katharina Ziolkowski (Tallinn: NATO CCD COE, 2013), 621.

Sandy Ghandhi, "Human Rights and the International Court of Justice," *Human Rights L. Rev.* 11 (2011): 527.

Terry D. Gill, "Non-Intervention in the Cyber Context," in *Peacetime Regime for State Activities in Cyberspace*, ed. Katharina Ziolkowski (Tallinn: NATO CCD COE, 2013), 217.

———. "International humanitarian law applied to cyber-warfare: Precautions, proportionality and the notion of 'attack' under the humanitarian law of armed conflict" in *Research Handbook on International Law and Cyberspace*, eds. Nicholas Tsagourias and Russell Buchan (Cheltenham: Edward Elgar, 2015), 366.

Zachary K. Goldman, "Navigating Deterrence: Law, Strategy, and Security in the Twenty-First Century", *Int'l L. & Politics* 47 (2015): 311.

Jack Goldsmith and Tim Wu, *Who Controls the Internet?: Illusions of a Borderless World* (Oxford: Oxford University Press, 2006).

Jennifer Granick, "Changes to export control arrangement apply to computer exploits and more" (Stanford, CA: Center for Internet and Society, Stanford Law School, 15 Jan. 2014).

Christine Gray, *International Law and the Use of Force*, 3rd ed. (Oxford: Oxford University Press, 2008).

Christopher Greenwood, "International Law and the Pre-Emptive Use of Force: Afghanistan, Al-Qaida, and Iraq," *San Diego Int'l L. J.* 4 (2003): 7.

Matthew J. Greer, "Redefining Perfidy," *Georgetown JIL* 47 (2015): 241.

Hugo Grotius, *De Jure Belli Ac Pacis Libris Tres* (Indianapolis: Bobbs-Merrill, Francis W. Kelsey trans., 1925).

Serge Gutwirth *et al.*, eds., *European Data Protection: In Good Health?* (Dordrecht: Springer, 2012).

Nikolas K. Gvosdev, "The Bear Goes Digital: *Russia and Its Cyber Capabilities*," in *Cyber Challenges and National Security: Threats, Opportunities, and Power in a Virtual World*, ed. Derek S. Reveron (Washington, DC: Georgetown University Press, 2012), chap. 11.

Monica Hakimi and Jacob Katz Cogan, "The Two Codes on the Use of Force", *Euro. J. Int'l L* 27 (2016): 257.

Manny Halberstram, "Hacking Back: Reevaluating the Legality of Retaliatory Cyberattacks," *Geo. Wash. Int'l L. Rev.* 46 [2013]: 199.

Noah C.N. Hampson, "Hacktivism: A New Breed of Protest in a Networked World," *Boston Coll. Int'l & Comp. L. Rev.* 35 (2012): 511.

Harvard Program on Humanitarian Policy and Conflict Research (HPCR), *Manual on International Law Applicable to Air and Missile Warfare* (Cambridge, MA: Harvard University, 2009).

Oona A. Hathaway and Rebecca Crootof, "The Law of Cyber-Attack," *Calif. L. Rev.* 100 (2012): 817.

Jean-Marie Henckaerts and Louise Doswald-Beck, eds., *Customary International Humanitarian Law* (Cambridge: Cambridge University Press, 2005).

Mireille Hildebrandt, "Legal and technological normativity: more (and less) than twin sisters", *Techné: Research in Philosophy and Technol.* 12 (2008): 169.

Mahmoud Hmoud, "Are New Principles Really Needed? The Potential of the Established Distinction between Responsibility for Attacks by Non-State Actors and the Law of Self-Defence," *Amer. JIL* 107 (2013): 576.

Gerritt Hornung and Christoph Schnabel, "Data Protection in Germany I: The population census decision and the right to information self-determination," *Computer L. & Security Rep.* 25 (2009): 84.

Peter Hustinx, "The Reform of EU Data Protection: Towards more effective and more consistent data protection access across the EU," in *Le développement du droit européen en matière de protection des données et ses implications pour la Suisse*, eds. Astrid Epiney and Tobias Fasnacht (Zurich: Schulthess, 2012), 15.

Nigel Inkster, "China in Cyberspace," *Cyber Challenges and National Security: Threats, Opportunities, and Power in a Virtual World*, ed. Derek S. Reveron (Washington, DC: Georgetown University Press, 2012), chap. 12.

International Committee of the Red Cross, "How is the Term 'Armed Conflict' Defined in International Humanitarian Law?", Opinion Paper, Mar. 2008.

———. *How Does Law Protect in War?* (Geneva: ICRC, 2012).

———. *International humanitarian law and the challenges of contemporary armed conflicts* (Geneva: ICRC, 2015).

The Internet Society, *Unleashing the Potential of the Internet for ASEAN Economies* (Washington, DC: Internet Society, 2015).

Emilio Iasiello, "Is Cyber Deterrence an Illusory Course of Action?", *J. Strat. Security* 7 (2014):52.

Eduard Ivanov, "Combating Cyberterrorism under International Law," *Baltic YBIL* 14 (2014): 55.

Agnieszka Jachec-Neale, *The Concept of Military Objectives in International Law and Targeting Practice* (London/New York: Routledge, 2015).

Maziar Jamnejad and Michael Wood, "The Principle of Non-intervention," *Leiden JIL* 22 (2009): 345.

Eric Talbot Jensen, "Cyber Deterrence", *Emory IL Rev.* 26 (2012): 773.

Marina Kaljurand, "United Nations Group of Government Experts: The Estonian Perspectives," in *International Cyber Norms: Legal, Policy & Industry* Perspectives, eds. Anna-MariaOsula and Henry Rõigas (Tallinn: NATO CCD COE, 2016), Chap. 6.

Philipp Kastner and Frédéric Mégret, "International Legal Dimensions of Cybercrime" in *Research Handbook on International Law and Cyberspace*, eds. Nicholas Tsagourias and Russell Buchan (Cheltenham: Edward Elgar, 2015), 190.

Rajbir Kaur, M.S. Kaur, Lalith Suresh and V. Laxmi, "DoS Attacks in MANETs: Detection and Countermeasures," in *Cyber Security, Cyber Crime and Cyber Forensics: Application and Perspectives*, eds. Raghu Santanam, M. Sethumadhavan and Mohit Virendra (Hershey, NY: Information Science Reference, 2011), chap. 10.

Camino Kavanagh and Daniel Stauffacher, *A Role for Civil Society: ICTs, Norms and Confidence Building Measures in the Context of International Security* (Geneva: ICT4Peace Foundation. 2014).

Jacob Kellenberger, President of the ICRC, "International Humanitarian law and New Weapon Technologies" (keynote address, 34th Roundtable on Current Issues of International Humanitarian Law, San Remo, 8–10 Sept. 2011).

Orin S. Kerr, "The Fourth Amendment and the Global Internet," *Stanford. L. Rev*. 67 (2015): 285.

Georg Kerschischnig, *Cyberthreats and International Law* (The Hague: Eleven Publishing, 2012).

Nancy J. King and V.T. Raja, "What Do They Really Know About Me in the Cloud? A Comparative Law Perspective on Protecting Privacy and Security of Sensitive Consumer Data," *Am. Bus. L.J.* 50 (2013): 413.

Jan Klabbers, "Responsibility of States and International Organizations in the Context of Cyber Activities with Special reference to NATO," in *Peacetime Regime for State Activities in Cyberspace*, ed. Katharina Ziolkowski (Tallinn: NATO CCD COE, 2013), 485.

Alexander Klimburg, ed., *National Cyber Security Framework Manual* (Tallinn: NATO CCD COE Publication, 2012).

Harold Koh (Legal Avisor, US Dept. of State), "International Law in Cyberspace" (paper presented at the US CYBERCOM Inter-Agency Legal Conference, Ft. Meade, MD, 18 Sept. 2012).

Uta Kohl, "Jurisdiction in cyberspace," in *Research Handbook on International Law and Cyberspace*, eds. Nicholas Tsagourias and Russell Buchan (Cheltenham : Edward Elgar, 2015). 30.

J. Kokott and C.Sobotta, "The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR," *International Data Privacy Law* 3 (2013): 222.

Eugene Kontorovich, "The Piracy Analogy: Modern Universal Jurisdiction's Hollow Foundation." *Harvard ILJ* 45 (2004): 183.

Dimitrios Koukiadis, *Reconstituting Internet Normativity: The role of State, private actors, global online community in the production of legal norms* (Baden-Baden: Nomos, 2015).

Krystyna Kowalik-Bańczyk, "Les aspects transforntaliers des infractions à la vie privée par la surveillance de masse de la part des agences étatiques," *Revue générale du droit international public* 119 (2015): 383.

Dino Kritsiotis, "A study of the concept and operation of the rights of individual and collective self-defence under international law," in *Research Handbook on International Conflict and Security Law:* Jus ad Bellum, Jus in Bello, *and* Jus post Bellum, eds. Nigel D. White and Christian Henderson (Cheltham: Edward Elgar, 2013), chap. 6.

Joanna Kulesza, *International Internet Law* (London and New York: Routledge, 2012).

Christopher Kuner, "An international legal framework for data protection: Issues and prospects," *Computer Law & Security Rev.* 25 (2009): 307.

———. "Data Protection Law and the International Jurisdiction on the Internet (Part 2)," *Int'l J. Law & Information Techno.* 18 (2010): 225.

———. "Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present and Future," *OECD Digital Economy Papers*, No. 187, OECD Publishing (2011).

———. "The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law," *Privacy & Security L. Rep.*, 11 PVLR 06, 02/06/2012.

———. *Transborder Data Flows and Data Privacy Law* (Oxford: Oxford University Press, 2013).

———. "The European Union and the Search for an International Data Protection Framework," *Groningen JIL* 2 (2014): 55.

———. "The Court of Justice of the EU Judgment on Data Protection and Internet Search Engines: Current Issues and Future Challenges," *Studies of the Max Planck Institute Luxembourg for International, European & Regulatory Procedural Law* (Ashgate: Nomos/Brill, 2015).

———. "Extraterritoriality and International Data Transfers in EU Data Protection Law," *University of Cambridge Legal Studies Research Paper Series No. 49/2015* (Aug. 2015).

———. "Reality and Illusion in EU Data Transfer Regulation Post Schrems," *University of Cambridge Fac. of Law Research Paper* (14 Feb. 2016).

Christopher Kuner, Cédric Burton, and Anna Pateraki, "The Proposed EU Data Protection Regulation Two Years Later," *Privacy & Security L. Rep.*, 13 PVLR 8, 01/06/2014.

Jovan Kurbalija, "E-Diplomacy and Diplomatic Law in the Internet Era," in *Peacetime Regime for State Activities in Cyberspace*, ed. Katharina Ziolkowski (Tallinn: NATO CCD COE, 2013), 393.

Newton Lee, *Counterterrorism and Cybersecurity: Total Information Awareness*, 2nd ed. (New York: Springer, 2015).

Genevieve Lennon and Clive Walker, eds., *Routledge Handbook of Law and Terrorism* (London and New York: Routledge, 2015).

Daniel Adeoyé Leslie, *Legal Principles for Combating Cyberlaundering* (Dordrecht/New York: Springer, 2014).

Lawrence Lessig, *Code and Other Laws of Cyberspace* (New York: Basic Books, 1999).

———. "Code IS Law: On Liberty in Cyberspace", *Harvard Magazine* (Jan. 2000).

———. *CODE Version 2.0* (New York: Basic Books, 2006).

Claire Levallois-Barth, *Sensitive data protection in the European Union* (Brussels: Bruylant, 2007).

James A Lewis, *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats* (Washington, DC: Center for Strategic & International Studies, 2002).

Martin C. Libicki, *Crisis and Escalation in Cyberspace* (Santa Monica, CA: RAND, 2012).

Thomas R. Lifeländer, "The *Lubanga* Judgment of the ICC: More Than Just the First Step?," *Cambridge J. Int'l & Comp. L.* 1 (2012): 191.

Samuel P. Liles III, "Cyber Warfare as a Form of Conflict: Evaluation of Models of Cyber Conflict as a Prototype to Conceptual Analysis", Ph.D. thesis, Purdue University, 2012.

Herbert Lin, "Cyber conflict and international humanitarian law," *International Rev. Red Cross* 94 (2012): 515.

David Livingtone and Patricia Lewis, *Space, the Final Frontier for Cybersecurity?* (London: Chatham House, 2016).

Arno R. Lodder, "Conflict resolution in virtual worlds: General characteristics and the 2009 Dutch convictions on virtual theft," in *Virtual worlds and criminality*, eds. K. Cornelius and D. Hermann (Berlin: Springer, 2011), 79.

Stuart Macdonald, "Dataveillance and terrorism: Swamps, haystacks and the eye of providence," in *Routledge Handbook of Law and Terrorism*, eds. Genevieve Lennon and Clive Walker (London and New York: Routledge, 2015), 147.

Himanshu Maheshwari, H.S. Hyman, and Manish Agrawal, "A Comparison of Cyber-Crime Definitions in India and the United States," in *Cyber Security, Cyber Crime and Cyber Forensics: Application and* Perspectives, eds. Santanam, Sethumadhavan and Virendra (Hershey, NY: Information Science Reference, 2011), chap. 3.

Marina Mancini, Faustin Z. Ntoubandi, and Thilo Marauhn, "Old Concepts and New Challenges?: Are Private Contractors the Mercenaries of the Twenty-first Century?," in *War by Contract: Human Rights, Humanitarian Law, and Private Contractors*, eds. Francesco Francioni and Natalino Ronzitti (Oxford: Oxford University Press, 2011), chap. 16.

Peter Margulies, "Sovereignty and Cyber Attacks: Technology's Challenge to the Law of State Responsibility," *Melbourne JIL* 14 (2013): 496.

Martha Mejía-Kaiser, "Space Law and Unauthorized Cyber Activities," in *Peacetime Regime for State Activities in Cyberspace*, ed. Katharina Ziolkowski (Tallinn: NATO CCD COE, 2013), 349.

Nils Melzer, *Interpretative guidance on the notion of direct participation in hostilities under international humanitarian law* (Geneva: ICRC, 2009).

———. *Cyberwarfare and International Law* (Geneva: UNIDIR Resources, 2011).

Samantha Miko, "*Al-Skeini v. United Kingdom* and Extraterritorial Jurisdiction under the European Convention for Human Rights," *Boston Coll. Int'l & Comp. L. Rev.* 35 (2013): 63.

Marko Milanovic, *Extraterritorial Application of Human Rights Treaties: Law, Principles, and Policy* (Oxford: Oxford University Press, 2011).

———. "*Al-Skeini* and *Al-Jedda* in Strasbourg," *Euro. JIL* 23 (2012): 121.

———. "Human Rights Treaties and Foreign Surveillance," *Harvard Int'l LJ* 56 (2015): 81.

Christopher Millard, ed., *Cloud Computing Law* (Oxford: Oxford University Press, 2013).

Andrew D. Mitchell and Glyn Ayres, "General and Security Exceptions Under the GATT and the GATS," in *International Trade Law and WTO*, eds. Indira Carr, Jahid Bhuiyan, and Shawkat Alam (Annandale, NSW, Australia: Federation Press, 2012).

Lindsay Moir, *Reappraising the Resort to Force: International Law,* Jus ad Bellum *and the War on Terror* (Oxford: Hart Publishing, 2010).

James Mulcahy and Charles O. Mahony, "Anticipatory Self-Defence: A Discussion of the International Law," *Hanse Law Rev.* 2 (2006): 231.

A. Sam Muller, *International Organizations and Their Host States: Aspects of Their Legal Relationship* (The Hague: Kluwer, 1995).

Sean D. Murphy, "The Doctrine of Preemptive Self-Defense," *Villanova L. Rev.* 50 (2005): 699.

T. Murphy and G.O. Cuinn, "Works in Progress: New Technologies and the European Court of Human Rights," *Hum. Rts. L. Rev.* 10 (2010): 601.

Eric Myjer, "Some Thoughts on Cyber Deterrence and Public International Law," in *Research Handbook on International Law and Cyberspace*, eds. Nicholas Tsagourias and Russell Buchan (Cheltenham : Edward Elgar, 2015), 284.

Hitoshi Nasu and Helen Trezise, "Cyber Security in the Asia-Pacific," in *Research Handbook on International Law and Cyberspace*, eds. Nicholas Tsagourias and Russell Buchan (Cheltenham: Edward Elgar, 2015), 446.

Dawn C. Nunziato, "The Beginning of the End of Internet Freedom," *Georgetown J. Int'l L.* 45 (2014): 383.

Mary Ellen O'Connell, "The prohibition of the use of force," in *Research Handbook on International Conflict and Security Law:* Jus ad Bellum, Jus in Bello, *and* Jus post Bellum, eds. Nigel D. White and Christian Henderson (Cheltenham: Edward Elgar:2013), chap. 4.

Anna-Maria Osula and Henry Rõigas, eds., *International Cyber Norms: Legal, Policy & Industry Perspectives* (Tallinn: NATO CCD COE, 2016).

Suleyman Ozeren, Ismail Dincer Gunes, and Diab M. Al-Badayneh, eds., *Understanding Terrorism: Analysis of Sociological and Psychological Aspects* (Amsterdam: IOS Press, 2007).

Jordan J. Paust, " Can You Hear Me Now?: Private Communication, National Security, and Human Rights Disconnect," *Chicago JIL* 15 (2015): 615.

———. "Operationalizing Use of Drones Against Non-State Terrorists Under the International Law of Self-defense," *Albany Govt. L. Rev.* 8 (2015): 166.

———. "NIAC Nonsense, the Afghan War, and Combatant Immunity," *Ga. J. Int'l & Comp. L.* 44 (2016) (forthcoming).

Cheryl Pellerin, "DARPA Plan X Uses New Technologies to 'See' Cyber Effects", (American Forces Press Service, US Dept. of Defence, 11 Jun. 2014).

Wolter Pieters, Dina Hadziosmanovic, and Francien Dechesne, "Security-By-Experiment: Lessons from Responsible Deployment in Cyberspace", *Sci. Eng. Ethics* 22 (2016): 831.

Mauno Pihelgas, "Back-Tracing and Anonymity in Cyberspace," in *Peacetime Regime for State Activities in Cyberspace*, ed. Katharina Ziolkowski (Tallinn: NATO CCD COE, 2013), 31.

Benedikt Pirker, "Territorial Sovereignty and Integrity and the Challenges of Cyberspace," in *Peacetime Regime for State Activities in Cyberspace,* ed. Katharina Ziolkowski (Tallinn: NATO CCD COE, 2013), 189.

Jompon Pitaksantayothin, "Cyber Terrorism Laws in the United States, the United Kingdom and Thailand: A Comparative Study," *Chulalongkorn Law Journal* 32 (2014): 169.

Dinah PoKempner, "Cyberspace and State Obligations in the Area of Human Rights," in *Peacetime Regime for State Activities in Cyberspace,* ed. Katharina Ziolkowski (Tallinn: NATO CCD COE, 2013), 239.

Yaroslav Radziwill, *Cyber-Attacks and the Exploitable Imperfections of International Law* (Leiden/Boston: Brill, 2015).

Ezekiel Rediker, "The Incitement of Terrorism on the Internet: Legal Standards, Enforcement, and the Role of the European Union," *Michigan JIL* 36 (2015): 321.

Chris Reed, *Making Laws for Cyberspace* (Oxford: Oxford University Press, 2012).

Derek S. Reveron, ed., *Cyber Challenges and National Security: Threats, Opportunities, and Power in a Virtual World* (Washington, DC: Georgetown University Press, 2012).

Adam Roberts, "The Laws of War: Problems of Implementation in Contemporary Conflicts," *Duke J. Comp. & IL* 6 (1995): 11.

Marco Roscini, *Cyber Operations and the Use of Force in International Law* (Oxford: Oxford University Press, 2014).

———. "Cyber Operations as a Use of Force," in *Research Handbook on International Law and Cyberspace*, eds. Nicholas Tsagourias and Russell Buchan (Cheltenham: Edward Elgar, 2015), 233.

Neil C. Rowe, "Distinctive Ethical Challenges of Cyberweapons," in *Research Handbook on International Law and Cyberspace*, eds. Nicholas Tsagourias and Russell Buchan (Cheltenham: Edward Elgar, 2015), 307.

Lambèr Royakkers and Rinie van Est, "The crucible warrior: the marionette of digitalized warfare", *Ethics Inf. Technol.* 12 (2010): 289.

Alexander Rust, "Data Protection as a Fundamental Right," in *Exchange of Information and Bank Secrecy*, eds. Alexander Rust and Eric Fort (Alphen aan den Rijn: Wolters Kluwer, Law & Business, 2012), chap. 10.

Tom Ruys, *'Armed Attack' and Article 51 of the UN Charter: Evolutions in Customary Law and Practice* (Cambridge: Cambridge University Press, 2010).

———. "The Meaning of 'Force' and the Boundaries of the *Jus Ad Bellum*: Are 'Minimal' Uses of Force Excluded from UN Charter Article 2(4)?," *Amer. JIL* 108 (2014): 159.

Leila Nadya Sadat, ed., *Forging a Convention for Crimes Against Humanity* (Cambridge: Cambridge University Press, 2011).

Marijin Sax, "Big data: Finders keepers, losers weepers?", *Ethics Inf. Technol.* 18 (2016): 25.

Ben Saul, "Legislating from a Radical Hague: The UN Special Tribunal for Lebanon Invents an International Crime of Transnational Terrorism," *Leiden JIL* 24 (2011): 677.

Ben Saul and Kathleen Heath, "Cyber Terrorism," in *Research Handbook on International Law and Cyberspace*, eds. Nicholas Tsagourias and Russell Buchan (Cheltenham: Edward Elgar, 2015), 147.

Arie J. Schaap, "Cyber Warfare Operations: Development and Use under International Law," *Air Force L. Rev.* 64 (2009): 121.

Scott J. Schackelford, *Managing cyber attacks in international law, business, and relations: In search of cyber peace* (Cambridge: Cambridge University Press, 2014).

Michael P. Scharf and Michael A. Newton, "Terrorism and Crimes Against Humanity," in *Forging a Convention for Crimes Against Humanity*, ed. Leila Nadya Sadat (Cambridge: Cambridge University Press, 2011), 262.

Michael N. Schmitt, " Wired warfare: Computer network attack and *jus in bello*," *International Rev. Red Cross* 84 (2002): 365.

———. "Cyber Operations and the *Jus Ad Bellum* Revisited," *Villanova L. Rev.* 56 (2011): 569.

———. "International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed," *Harvard Int'l LJ.* 54 (2012): 13.

———. "Classification of cyber conflict," *J. Conflict & Security L.* 17 (2012): 245.

———. "Cyber Activities and the Law of Countermeasures," in *Peacetime Regime for State Activities in Cyberspace*, ed. Katharina Ziolkowski (Tallinn: NATO CCD COE, 2013), 659.

———. ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge: Cambridge University Press, 2013).

———. "In Defense of Due Diligence in Cyberspace," *Yale Law Journal Forum* 125 (2015): 68.

Michael N. Schmitt and Brian T. O'Donnell, eds., *Computer Network Attack and International Law* (New Port, Rhode Island: US Naval War College International Law Studies, 2002).

Michael N. Schmitt and M. Christopher Pitts, "Cyber Countermeasures and Effects on Third Parties: The International Legal Regime," *Baltic YBIL* 14 (2014): 1.

Jürg Schneider and Monique Sturny, "Switzerland," *The Privacy, Data Protection and Cybersecurity Law Review* 2 (2015): Chapter 24.

Bruce Schneier, *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World* (New York: W.W. Norton, 2015).

Victor S. Seleznev, Alexey V. Liseikin, Alexey A. Bryskin, and Pavel V. Gromyko, "What Caused the Accident at the Sayano-Shushenskaya Hydroelectric Power Plant (SSHPP): A Seismologist's Point of View," *Seismological Research Letters* 85 (2014): 817.

Antonio Segura Serrano, "Cybersecurity: towards a global standard in the protection of critical information infrastructures," *Euro. J. Law & Techno.* 6 (2015): 1.

Daniel Severson, "American Surveillance of Non-U.S. Persons: Why New Privacy Protections Offer Only Cosmetic Change," *Harvard ILJ* 56 (2015): 465.

Jonathan Shaw, "The Watchers: Assault on privacy in America", *Harvard Magazine* (Jan.-Feb. 2017).

Aaron Shull, "Cyber Espionage and International Law" (paper presented at the *Global Internet Governance Academic Network* (GigaNet) Annual Symposium, Bali, 21 Oct. 2013).

P.W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs To Know* (New York: Oxford University Press, 2014).

Sajai Singh, Probir Roy Chowdhury, Amrut Joshi, and Govind Naidu, "Technology Surveillance," in *Legal Issues in the Global Information Society* , eds. Dennis Campbell and Chrysta Bán (Dobbs Ferry, NY: Oceana, 2005.), chap. 3.

Société Française pour le Droit International, *Colloque de Rouen: Internet et le droit international* (Paris: Editions A. Pedone, 2014).

Andrei Soldatov and Irina Borogan, *The Red Web: The Struggle Between Russia's Digital Dictators and the New Online Revolutionaries* (New York: Public Affairs, 2015).

D.J. Solove, "'I've Got Nothing to Hide' and Other Misunderstandings of Privacy," *San Diego L. Rev.* 44 (2007): 745.

Henrik Spang-Hanssen, *Cyberspace & International Law on Jurisdiction: Possibilities of Dividing Cyberspace into Jurisdictions with Help of Filters and Firewall Software* (Copenhagen: DJØF Publishing, 2004).

———. *Public International Computer Network Law Issues* (Copenhagen: DJØF Publishing, 2006).

Raymond E. Spier, "'Dual Use' and 'Intentionality': Seeking to Prevent the Manifestation of Deliberately Harmful Objectives", *Sci. Eng. Ethics* 16 (2010): 1.

Titus Stahl, "Indiscriminate mass surveillance and the public sphere", *Ethics Inf. Technol.* 18 (2016): 33.

Daniel Stauffacher and Camino Kavanagh, *Confidence Building Measures and International Cyber Security* (Geneva: ICT4Peace Foundation, 2013).

Tim Stephens, "International Criminal Law and the Response to International Terrorism," *University New South Wales Law J.* 27 (2004): 454.

Jemima Stratford and Tim Johnston, "The Snowden 'Revelations': Is GCHO Breaking the Law?," *Euro. Human Rights L. Rev.* 14 [2014]: 129.

Litska Strikwerda, "Theft of virtual items in online multiplayer computer games: an ontological and moral analysis", *Ethics Inf. Technol.* 14 (2012): 89.

David J. Stute, "Privacy Almighty?: The CJEU's Judgment in Google Spain SL v. AEPD," *Michigan JIL* 36 (2015): 649.

K. Stylianou, J. Venturini and N. Zingales, "Protecting user privacy in the Cloud: an analysis of terms of service", *Euro. J. Law & Techno* 6 (2015): 100.

Clare Sullivan, *Digital Identity* (Adelaide: University of Adelaide Press, 2011).

G. Sulmasy and J. Yoo, "Counterintuitive: Intelligence Operations and International Law," *Mich. J. Int'l L.* 28 (2006): 625.

M. Taddeo and L. Floridi, "The Debate on the Moral Responsibilities of Online Service Providers", *Sci. Eng. Ethics* 22 (2016): 1575.

Dire Tladi, "The Nonconsenting Innocent State: The Problem with Bethlehem's Principle 12", *Amer. JIL* 107 (2013): 570.

Joel P. Trachtman, "International Economic Law in the Cyber Arena" in *Peacetime Regime for State Activities in Cyberspace*, ed. Katharina Ziolkowski (Tallinn: NATO CCD COE, 2013), 373.

Rochelle E. Tractenberg et al., "Using Ethical Reasoning to Amplify the Reach and Resonance of Professional Codes of Conduct in Training Big Data Scientists", *Sci. Eng. Ethics* 21 (2015): 1485.

Nicholas Tsagourias, "The Legal Status of Cyberspace" in *Research Handbook on International Law and Cyberspace*, eds. Nicholas Tsagourias and Russell Buchan (Cheltenham : Edward Elgar, 2015), 13.

———. "Self-Defence against Non-state Actors: The Interaction between Self-Defence as a Primary Rule and Self-Defence as a Secondary Rule," *Leiden JIL* 29 (2016): 801.

Nicholas Tsagourias and Russell Buchan, eds., *Research Handbook on International Law and Cyberspace* (Cheltenham: Edward Elgar, 2015).

Mark Tunick, *Balancing Privacy and Free Speech: Unwanted attention in the age of social media* (London and New York: Routledge, 2015).

David Turns, "Cyber War and the Law of Neutrality," in *Research Handbook on International Law and Cyberspace*, eds. Nicholas Tsagourias and Russell Buchan (Cheltenham: Edward Elgar, 2015), 380.

UN Office on Drugs and Crime, *The Use of the Internet for Terrorist Purposes* (New York, United Nations, 2012).

———. *Comprehensive Study on Cybercrime* (New York: United Nations, 2013).

United States Government, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World* (Washington, DC, 2011).

Brandon Valeriano and Ryan Maness, "Persistent Enemy and Cyberwar: *Rivalry Relations in an Age of Information Warfare*," in *Cyber Challenges and National Security: Threats, Opportunities, and Power in a Virtual World*, ed. Derek S. Reveron (Washington, DC: Georgetown University Press, 2012), 140.

B. Van der Sloot, "Privacy in the Post-NSA Era: Time for a Fundamental Revision ?," *J. Intellectual Property Info. Techno. & E-Commerce L.* 5 (2014): 2–11.

Manuel J. Ventura, "Terrorism According to the Special Tribunal for Lebanon's *Interlocutory Decision on the Applicable Law*: A Defining Moment or a Moment of Defining?," *J. Int'l Crim. Justice* 9 (2011): 1021.

———. "Two Controversies in the Lubanga Trial Judgment of the ICC: The Nature of Co-perpetration's Common Plan and the Classification of the Armed Conflict" in *The War Report 2012*, ed. S. Casey-Maslen (Oxford: Oxford University Press, 2013), chap. 13.

Wolff Heintschel von Heinegg, "Protecting Critical Submarine Cyber Infrastructure: Legal Status and Protection of Submarine Communications Cables under International Law," in *Peacetime Regime for State Activities in Cyberspace*, ed. Katharina Ziolkowski (Tallinn: NATO CCD COE, 2013), 291.

Ian Walden, "International Communications Law, the Internet and the Regulation of Cyberspace" in *Peacetime Regime for State Activities in Cyberspace*, ed. Katharina Ziolkowski (Tallinn: NATO CCD COE, 2013), 261.

Sean Watts, "Cyber Law Development and the United States Law of War Manual" in *International Cyber Norms: Legal, Policy & Industry Perspectives*, eds. Anna-Maria Osula and Henry Rõigas (Tallinn: NATO CCD COE, 2016), 49.

Matthew C. Waxman, "Cyber-Attacks and the Use of Force: Back to the Future of Article 2 (4)," *Yale JIL* 36 (2011): 421.

Thomas Weatherall, "The Status of the Prohibition of Terrorism in International Law," *Georgetown JIL* 46 (2015): 589.

Amalie M. Weber, "The Council of Europe's Convention on Cybercrime," *Berkeley Technology Law J.* 18 (2003): 425.

Rolf H. Weber, *Realizing a New Golbal Cyberspace Framework: Normative Foundations and Guiding Principles* (Berlin: Springer, 2015).

George R.S. Weir and Stephen Mason, "The Sources of Digital Evidence," in *Electronic Evidence*, 3rd ed., ed. Stephen Mason (London: Butterworth, 2012), 1.

Nigel D. White and Christian Henderson, eds., *Research Handbook on International Conflict and Security Law:* Jus ad Bellum, Jus in Bello, *and* Jus post Bellum (Cheltenham: Edward Elgar: 2013).

Elizabeth Wilmshurst, ed., *Principles of International Law on the Use of Force by States in Self-Defence* (London: Royal Institute of International Affairs, 2005).

Richard Ashby Wilson, ed., *Human Rights in the 'War on Terror'* (Cambridge: Cambridge University Press, 2005).

Johann-Christoph Woltag, *Cyber Warfare: Military Cross-Border Computer Network* (Cambridge: Intersentia, 2014).

Andrew K. Woods, "Against Data Exceptionalism," *Stanford L. Rev.* 68 (2016): 729.

Ashlee Woods, "Terrorists and the Internet" in *Understanding Terrorism: Analysis of Sociological and Psychological Aspects*, eds. Suleyman Ozeren, Ismail Dincer Gunes, and Diab M. Al-Badayneh (Amsterdam: IOS Press, 2007), 270.

Pål Wrange, "Intervention in National and Private Cyberspace and International Law," in *International Law and Changing Perceptions of Security: Liber Amicorum Said Mahmoudi*, eds. J. Ebbesson *et al.* (Leiden/Boston: Brill Nijhoff, 2014), 307.

Tim Wu, Esther Dyson, Michael Froomkin, and David Gross, "On the Future of Internet Governance", *Amer. Soc. IL Proc.* 101 (2007): 201.

Tim Wu, *The Master Switch: The Rise and Fall of Information Empires* (New York: Knopf Doubleday, 2011).
Joachim Zekoll, "Online Dispute Resolution: Justice without the State?," *Max Planck Institute for European Legal History Research Paper* Series No. 2014–02.
Huang Zhxiong, "The Attribution Rules in ILC's Articles on State Responsibility: A Preliminary Assessment on Their Application to Cyber Operations," *Baltic YBIL* 14 (2014): 41.
Andreas Zimmermann, "International Law and 'Cyber Space'," *European Soc. International Law Reflections* 3 (2014): 1.
Katharina Ziolkowski, ed., *Peacetime Regime for State Activities in Cyberspace* (Tallinn: NATO CCD COE, 2013).
———. "Peacetime Cyber Espionage – New Tendencies in Public International Law" in ibid., 425.
———. "Confidence Building Measures for Cyberspace" in ibid., 533.
Jonathan Zittrain, *The Future of the Internet And How to Stop It* (New Haven: Yale University Press, 2008).

Internet Resources

Апетьян: Это продолжение линии властей ЕС на регулирование Интернета [Apetyan: This is the continuation of the EU government's policy to regulate the Internet], available at http://vz.ru/news/2014/6/4/690049.html.
Cordula Droege (ICRC Legal Adviser), "No legal vacuum in cyber space", Interview on 16 Aug. 2011, *ICRC Resource Centre*, available at: https://www.icrc.org/eng/resources/documents/interview/2011/cyber-warfare-interview-2011-08-16.htm.
European Union, Joint Statement of the ministers of interior and justice of 11 European States dated 11 Jan. 2015, available at: http://ec.europa.eu/dgs/home-affairs/what-is-new/news/news/docs/20150111_joint_statement_of_ministers_for_interrior_en.pdf.
Facebook, *Global Government Requests Report*, available at: https://govtrequests.facebook.com/
Freedom House's *Freedom on the Net 2015*, available at: https://freedomhouse.org/report/freedom-net/freedom-net-2015.
Laurent Gisel (ICRC Legal Adviser), "The law of war imposes limits on cyber attacks too", Interview on 1 Jul. 2013, available at: https://www.icrc.org/eng/resources/documents/interview/2013/06-27-cyber-warfare-ihl.htm.
Human Rights Committee, *Concluding Observations on the Fourth Report of the United States of America*, para. 9 (26 Mar. 2014), available at: http://justsecurity.org/wp-content/uploads/2014/03/UN-ICCPR-Concluding-Observations-USA.pdf.
International Committee of the Red Cross, Advisory Service on International Humanitarian Law, *What is International Humanitarian Law?* (Geneva: ICRC, Jul. 2004), p. 1, available at: https://www.icrc.org/eng/assets/files/other/what_is_ihl.pdf.
———. "What limits does the law of war impose on cyber attacks? Questions and answers," 28 Jun. 2013, available at: https://www.icrc.org/eng/resources/documents/faq/130628-cyber-warfare-q-and-a-eng.htm.
———. Updated Commentary to the First Geneva Convention of 1949 (2016), available at: https://www.icrc.org/ihl/full/GCi-commentary.
Ifex, "How "The Right to be Forgotten" affects privacy and free expression", 21 Jul. 2014, available at: https://www.ifex.org/europe_central_asia/2014/07/21/right_forgotten/.
Internet World Stats, available at: http://www.internetworldstats.com/stats.htm.
Internet World Stat, *Usages and Population Statistics*, available at: http://www.internetworldstats.com/top20.htm.

La Quadrature du Net, "The Right to be Forgotten: Don't Forget the Rule of Law!", 17 Jul. 2014, available at: https://www.laquadrature.net/en/the-right-to-be-forgotten-dont-forget-the-rule-of-law.

Liberty and Security in a Changing World, Report and Recommendations of the [US] President's Review Group on Intelligence and Communications Technologies (12 Dec. 2013), available at: http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

Joel Macharia, "Africa Needs a Cyber Security Law But AU's Proposal is Flawed, Advocates Say", *techPresident*, 31 Jan. 2014, available at: http://techpresident.com/news/wegov/24712/africa-union-cybersecurity-law-flawed.

Marko Milanovic, "Foreign Surveillance and Human Rights, Part 4: Do Human Rights Treaties Apply to Extraterritorial Interferences With Privacy?" (2013), available at: http://www.ejiltalk.org/foreign-surveillance-and-human-rights-part-4-do-human-rights-treaties-apply-to-extraterritorial-interferences-with-privacy/.

Memorandum for Chiefs of the Military Services, Commanders of the Combatant Commands, and Directors of the Joint Staff Directorate, available at: http://www.nsci-va.org/CyberReferenceLib/2010-11-joint%20Terminology%20for%20Cyberspace%20Operations.pdf.

NATO Standardization Agency (NSA), *NATO Glossary of Terms and Definitions* (AAP-6 of 2013) 2-C-11, available at: http://nsa.nato.int/nsa/zPublic/ap/aap6/AAP-6.pdf.

Necessary and Proportionate, "International Principles on the Application of Human Rights Law to Communications Surveillance – Background and Supporting International Legal Analysis", May 2014, available at: https://necessaryandproportionate.org/legalanalysis.

Anne Peters, "Surveillance Without Borders? The Unlawfulness of the NSA-Panopticon, Part I" (2013),availableat:http://www.ejiltalk.org/surveillance-without-borders-the-unlawfulness-of-the-nsa-panopticon-part-i/.

———. "Surveillance without Borders? The Unlawfulness of the NSA Panopticon, Part II" (2013),availableat:http://www.ejiltalk.org/surveillance-without-borders-the-unlawfulness-of-the-nsa-panopticon-part-ii/.

Privacy International, *The Global Surveillance Industry*, Jul. 2016, available at: https://privacyinternational.org/sites/default/files/global_surveillance.pdf.

Safeguarding National Security (Section 24 of the Freedom of Information Act), available at: http://ico.org.uk/for_organisations/guidance_index/~/media/documents/library/Freedom_of_Information/Detailed_specialist_guides/safeguarding_national_security_section_24_foi.ashx.

Joran Spauwen and Jens van den Brink, "Dutch Google Spain ruling: More Freedom of Speech, Less Right To Be Forgotten For Criminals", *Meld je nu aan voor de Media Report Nieuwsbrief!* (24 Sept. 2014), available at: http://www.mediareport.nl/persrecht/26092014/google-spain-judgment-in-the-netherlands-more-freedom-of-speech-less-right-to-be-forgotten-for-criminals/.

Stein Schjolberg, *The Third Pillar in Cyberspace: An International Court or Tribunal for Cyberspace*, available at: http://www.cybercrimelaw.net/documents/131112_Draft_Treaty_text_on_International_Criminal_Tribunal_for_Cyberspace.pdf.

TeleGeography's interactive Submarine Cable Map 2014, available at: https://www.telegeography.com/telecom-resources/submarine-cable-map/index.html.

Twitter, *Transparency Report*, available at:https://transparency.twitter.com/.

US Intelligence Community, "Background to 'Assessing Rusian Activities and Intentions in Recent US Elections': The Analytic Process and Cyber Incident Attribution" (6 Jan. 2017), available at: https://www.dni.gov/files/documents/ICA_2017_01.pdf.

Rolf H. Weber, "Proliferation of Internet Governance: (1 Sept. 2014)". GigaNet Governance Academic Network, Annual Symposium 2014, available at: http://dx.doi.org/10.2139/ssrn.2809874.

Alan Wehler, "The Future of EU Data Protection: Challenges in light of PRISM", 3 Oct. 2013, available at: http://safegov.org/2013/10/3/the-future-of-eu-data-protection-challenges-in-light-of-prism.

Other Documents

Letter from Daniel Webster to Lord Ashburton dated 6 Aug. 1842, *reprinted* in 2 *Int'l L. Digest* 412 (ed. John Bassett Moore, 1906); K.E. Shewmaker (ed.), *The Papers of Daniel Webster: Diplomatic Papers, vol. 1: 1841–1843* (Armidale: University of New England Press, 1983), p. 62.

Declaration Renouncing the Use, in Time of War, of Explosive Projectiles Under 400 Grammes Weight, Nov. 29/Dec. 11, 1868 ("1868 St. Petersburg's Declaration") 18 *Martens Nouveau Recueil* (ser. 1) 474.

Human Rights Committee, *Celiberti de Casariego v. Uruguay*, 29 July 1981, Communication no. 56/1979.

———. *Lopez Burgos v. Uruguay*, Communication No. R.12/52, U.N. Doc. Supp. No. 40 (A/36/40) at 176 (1981).

———. *ICCPR General Comment no. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation*, 8 April 1988.

———. *Toonen v Australia*, 25 Dec. 1991, Communication No. 488/1992.

———. *Antonius Cornelis Van Hulst v. Netherlands*, 8 Apr. 1998, Communication No. 903/1999.

———. *General Comment no. 31, The nature of the general legal obligation imposed on States Parties to the Covenant*, 26 May 2004, CCPR/C/21/Rev.1/Add.13.

———. *ICCPR General Comment no. 34, Article 19, Freedoms of opinion and expression*, 12 Sept. 2011, CCPR/C/GC/34.

Council of Europe, *Explanatory Report on the Convention on Cybercrime* (ETS No. 185) (2001).

The National Security Strategy of the United States (Washington, DC: Office of the White House, 2002).

Inter-American Juridical Committee of the OAS, "Personal Data Protection", Doc. CJI/RES. 186 (LXXX-O/12).

Joint Chiefs of Staff, US Dept. of Defense, Joint Pub. 3–13, *Information Operations* (13 Feb. 2006).

Draft Preliminary Principles and Recommendations on Data Protection (the Protection of Personal Data), Permanent Council of the Organization of American States, Committee on Juridical and Political Affairs, OEA/Ser.G CP/CAJP-2921/10, 19 Nov. 2010.

Initial Set of OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies, OSCE Permanent Council Decision No. 1106 (PC.DEC/1106).

Office of the National Counterintelligence Executive, *Foreign Spies Stealing US Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009–2011* (Washington, DC: Office of the Director of National Intelligence, Oct. 2011).

Draft international code of conduct for information security, UNGA Doc. A/66/359 (14 Sept. 2011).

UK Government, *The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world* (Nov. 2011).

Global Principles on National Security and the Right to Information ("The Tshwane Principles") (New York: Open Society Foundations, 2013).

Telecommunications Industry Dialogue on Freedom of Expression and Privacy of 12 Mar. 2013.

Statement of Heads of State or Government [of the European Union Member States] annexed to Doc. EUCO 169/13 dated 25 Oct. 2013.

US President's Review Group on Intelligence and Communications Technologies, *The NSA Report: Liberty and Security in a Changing World* (Dec. 2013).

US President's Executive Order "Improving Critical Infrastructure Cybersecurity", 12 Feb. 2013.

US President Barak Obama, *Remarks on Review of Signals Intelligence*, 17 Jan. 2014.

The Federal Government's Track Record on Cybersecurity and Critical Infrastructure, a report prepared by the Minority Staff of the Homeland Security and Government Affairs Committee, US Senate (4 Feb. 2014).

Intelligence and Security Committee of Parliament (UK), *Report on the intelligence relating to the murder of Fusilier Lee Rigby* (25 Nov. 2014).

UK Parliamentary Report, "The Darknet and Online Anonymity" (9 Mar. 2015).

US President's Cybersecurity National Action Plan (9 Feb. 2016).

Cybercrime Convention Committee (T-CY) Cloud Evidence Group, *Criminal justice access to electronic evidence in the cloud - Informal summary of issues and options under consideration by the Cloud Evidence Group* (17 Feb. 2016).

Joint Statement between the Presidents of China and Russia on Cooperation in Information Space Development dated 26 June 2016.

US President's Executive Order of 28 Dec. 2016, Taking Additional Steps to Address the National Emergency with Respect to Significant Malicious Cyber-Related Activities, Exec. Order No. 13757, 82 Fed. Reg. 1 (Dec. 28, 2016).