

Bibliography

- Liisi Adamson, 'Recommendation 13c', in Eneken Tikk (ed.), *Voluntary, Non-Binding Norms for Responsible State Behaviour in the Use of Information and Communications Technology – A Commentary* (United Nations Office for Disarmament Affairs 2017), 49–75
- Daniel Albrecht, 'Chinese Cybersecurity Law Compared to EU-NIS-Directive and German IT-Security Act', *Computer Law Review International* (2018), 1–5
- Anthony d'Amato, *The Concept of Custom in International Law* (Cornell University Press, 1971)
- Elif Askin, 'Economic and Social Rights, Extraterritorial Application', in Rüdiger Wolfrum (ed.), *Max Planck Encyclopedia of Public International Law* (Oxford: Oxford University Press 2019)
- Helmut Philipp Aust/Prisca Feihle, 'Due Diligence in the History of the Codification of the Law of State Responsibility', in Heike Krieger/Anne Peters/Leonhard Kreuzer, *Due Diligence in the International Legal Order* (Oxford: Oxford University Press 2020), 42–58
- Helmut Philipp Aust, 'Spionage im Zeitalter von Big Data – Globale Überwachung und der Schutz der Privatsphäre im Völkerrecht', *Archiv des Völkerrechts* 52 (2014), 375–406
- Björnstjern Baade, 'Due Diligence and the Duty to Protect Human Rights', in Heike Krieger/Anne Peters/Leonhard Kreuzer, *Due Diligence in the International Legal Order* (Oxford: Oxford University Press 2020), 92–108
- Björnstjern Baade, 'Fake News and International Law', *European Journal of International Law* 29 (2018), 1357–1376
- Björnstjern Baade, *Der Europäische Gerichtshof für Menschenrechte als Diskurswächter* (Berlin: Springer 2017)
- Jelena Bäumler, *Das Schädigungsverbot im Völkerrecht* (Berlin: Springer: 2017)
- Jelena Bäumler, 'Implementing the No Harm Principle in International Economic Law: A Comparison between Measure-Based Rules and Effect-Based Rules', *Journal of International Economic Law* 20 (2017), 807–828
- Christopher D. Baker, 'Tolerance of International Espionage: A Functional Approach', *American University International Law Review* 19 (2003), 1091–1113
- Karine Bannelier/Theodore Christakis, 'Prevention Reactions: The Role of States and Private Actors' (Paris: Les Cahiers de la Revue Défense Nationale 2017)
- Karine Bannelier-Christakis, 'Cyber Diligence: A Low-Intensity Due Diligence Principle for Low-Intensity Cyber Operations', *Baltic Yearbook of International Law* 14 (2014), 23–39

- Julio Barboza, 'International Liability for the Injurious Consequences of Acts Not Prohibited by International Law and Protection of the Environment', *Recueil des Cours de l'Académie de Haye* 247 (1998), 291–406
- Jens Bartelson, 'Dating Sovereignty', *International Studies Review* 20 (2018), 509–513
- Giulio Bartolini, 'The Historical Roots of the Due Diligence Standard', in Heike Krieger/Anne Peters/Leonhard Kreuzer (eds.), *Due Diligence in the International Legal Order* (Oxford: Oxford University Press 2020), 23–41
- Eyal Benvenisti, 'Community Interests in International Adjudication', in Eyal Benvenisti/Georg Nolte (eds.), *Community Interests Across International Law* (Oxford: Oxford University Press 2018), 70–85
- Michael Berk, 'Recommendations 13 (g) and (h)', in Eneken Tikk (ed.), *Voluntary, Non-Binding Norms for Responsible State Behaviour in the Use of Information and Communications Technology – A Commentary* (United Nations Office for Disarmament Affairs 2017), 191–222
- Antal Berkes, 'Human Rights Obligations of the Territorial State in the Cyberspace of Areas Outside Its Effective Control', *Israel Law Review* 52 (2019), 197–231
- Antal Berkes, 'The Standard of 'Due Diligence' as a Result of Interchange between the Law of Armed Conflict and General International Law', *Journal of Conflict & Security Law* 23 (2018), 433–460
- Samantha Besson, 'La Due Diligence en Droit International', *Recueil des Cours de l'Académie de Droit International de la Haye* 409 (2020) 153–398
- Samantha Besson, 'Sovereignty', in Rüdiger Wolfrum (ed.), *Max Planck Encyclopedia of Public International Law* (Oxford: Oxford University Press 2011)
- Alan E. Boyle, 'State Responsibility and International Liability for Injurious Consequences of Acts not Prohibited by International Law: A Necessary Distinction?', *International and Comparative Law Quarterly* 39 (1990), 1–26
- Jordan Branch, 'What's in a Name? Metaphors and Cybersecurity', *International Organization* 75 (2021), 39–70
- Dennis Broeders, *The Public Core of the Internet* (Amsterdam: Amsterdam University Press 2015)
- Gary Brown/Keira Poellet, 'The Customary International Law of Cyberspace', *Strategic Studies Quarterly* 6 (2012), 126–145
- Jutta Brunnée, 'Procedure and Substance in International Environmental Law', *Recueil des Cours de l'Académie de Droit International de la Haye* 405 (2020), 77–240
- Jutta Brunnée/Stephen J. Toope, *Legitimacy and Legality in International Law* (Cambridge: Cambridge University Press 2010)
- Russell Buchan, *Cyber Espionage and International Law* (Oxford: Hart Publishing 2018)
- Russell Buchan, 'The International Legal Regulation of Cyber Espionage', in Anna Maria Osula/Henry Röigas (eds.) *International Cyber Norms: Legal, Policy & Industry Perspectives* (NATO CCD COE Publications 2016), 65–86
- Russell Buchan, 'Cyberspace, Non-State Actors and the Obligation to Prevent Transboundary Harm', *Journal of Conflict & Security Law* 21 (2016), 429–453

- Russell Buchan, 'Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions', *Journal of Conflict & Security Law* 17 (2012), 211–227
- Els de Busser, 'Recommendation 13d', in Eneken Tikk (ed.), *Voluntary, Non-Binding Norms for Responsible State Behaviour in the Use of Information and Communications Technology – A Commentary* (United Nations Office for Disarmament Affairs 2017), 77–94
- Christian Calliess/Ansgar Baumgarten, 'Cybersecurity in the EU The Example of the Financial Sector: A Legal Perspective', *German Law Journal* 21 (2020), 1149–1179
- Simon Chesterman, 'Secret Intelligence', in Rüdiger Wolfrum (ed.), *Max Planck Encyclopedia of Public International Law* (Oxford: Oxford University Press 2009)
- Luke Chircop, 'A Due Diligence Standard of Attribution in Cyberspace', *International and Comparative Law Quarterly* 67 (2018), 1–26
- Luke Chircop, 'Territorial Sovereignty in Cyberspace after Tallinn Manual 2.0', *Melbourne Journal of International Law* 20 (2019), 349–377
- Theodore Christakis/Fabien Terpan, 'EU–US negotiations on law enforcement access to data: divergences, challenges and EU law procedures and options', *International Data Privacy Law* 11 (2021), 81–106
- Jonathan Clough, 'A World of Difference: The Budapest Convention on Cybercrime and the Challenges of Harmonisation', *Monash University Law Review* 40 (2015), 698–736
- Talita de Souza Dias/Antonio Coco, *Cyber Due Diligence in International Law* (Print version: Oxford Institute for Ethics, Law and Armed Conflict 2021)
- Antonio Coco/Talita de Souza Dias, "'Cyber Due Diligence": A Patchwork of Protective Obligations in International Law', *European Journal of International Law* 32 (2021), 771–805
- Antonio Coco/Talita de Souza Dias/Tsvetelina van Benthem, 'Illegal: The SolarWinds Hack under International Law', *European Journal of International Law* 33 (2022), 1275–1286
- Gary P. Corn/Robert Taylor, 'Sovereignty in the Age of Cyber', *AJIL Unbound* 111 (2017), 207–212
- Olivier Corten, *The Law against War – The Prohibition on the Use of Force in Contemporary International Law* (Oxford: Hart 2010)
- James Crawford, *Brownlie's Principles of Public International Law* (Oxford: Oxford University Press 2019)
- James Crawford, *Brownlie's Principles of Public International Law*, 8th edition (Oxford: Oxford University Press 2012)
- Rebecca Crootof, 'International Cybertorts: Expanding State Accountability in Cyberspace', *Cornell Law Review* 103 (2018), 565–644
- Georg Dahm/Jost Delbrück/Rüdiger Wolfrum, *Völkerrecht vol 1/1 Die Grundlagen: Die Völkerrechtssubjekte* (2nd edition, Berlin: Walter de Gruyter 1989)
- François Delerue, *Cyber Operations and International Law* (Cambridge: Cambridge University Press 2020)

- François Delerue, 'Covid-19 and the Cyber Pandemic: A Plea for International Law and the Rule of Sovereignty in Cyberspace', in Tatána Jančárková/Lauri Lindström et al. (eds.), *Going Viral* (NATO CCDCOE 2021), 9–24
- Hollin Dickerson, 'Best Practices', in Rüdiger Wolfrum (ed.), *Max Planck Encyclopedia of Public International Law* (Oxford: Oxford University Press 2010)
- Oliver Dörr, 'Prohibition of Use of Force', in Rüdiger Wolfrum (ed.), *Max Planck Encyclopedia of Public International Law* (Oxford: Oxford University Press 2019)
- Julia Dornbusch, *Das Kampfführungsrecht im internationalen Cyberkrieg* (Baden-Baden: Nomos 2018)
- Pierre-Marie Dupuy/Cristina Hoss, 'Trail Smelter and Terrorism: International Mechanism to Combat Transboundary Harm', in Rebecca M. Bratspies/Russell A. Miller (eds.), *Transboundary Harm in International Law: Lessons from the Trail Smelter Arbitration* (Cambridge: Cambridge University Press 2006), 225–239
- Leslie-Anne Duvic-Paoli, *The Prevention Principle in International Environmental Law* (Cambridge: Cambridge University Press 2018)
- Dan Efrony/Yuval Shany, 'A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice', *The American Journal of International Law* 112 (2018), 583–657
- Isabel Feichtner, 'Community Interest', in Rüdiger Wolfrum (ed.), *Max Planck Encyclopedia of Public International Law* (Oxford: Oxford University Press 2007)
- David P. Fidler, 'Cyberspace, Terrorism and International Law', *Journal of Conflict & Security Law* 21 (2016), 475–493
- Martha Finnemore/Duncan B. Hollis, 'Constructing Norms for Global Cybersecurity', *American Journal of International Law* 110 (2016), 425–478
- Martha Finnemore/Kathryn Sikkink, 'International Norm Dynamics and Political Change', *International Organization* 52 (1998), 887–917
- Caroline E. Foster, *Science and the Precautionary Principle in International Courts and Tribunals. Expert Evidence, Burden of Proof and Finality* (Cambridge: Cambridge University Press 2011)
- Danielle Flonk/Markus Jachtenfuchs/Aanke S. Obendiek, 'Authority Conflicts in Internet Governance: Liberals vs. Sovereignists?', *Global Constitutionalism* 9 (2020), 364–386
- Wolfgang Friedman, *The Changing Structure of International Law* (London: Stevens 1964)
- Marco Gercke, 'The Slow Wake of A Global Approach Against Cybercrime', *Computer Law Review International* 5 (2006), 140–145
- Terry D. Gill, 'Non-intervention in the Cyber Context', in Katharina Ziolkowski (ed.) *Peacetime Regime for State Activities in Cyberspace* (NATO CCDCOE 2013), 217–238
- Oren Gross, 'Cyber Responsibility to Protect: Legal Obligations of States Directly Affected by Cyber-Incidents', *Cornell International Law Journal* 48 (2015), 481–511
- Kari Hakapää, 'Innocent Passage', in Rüdiger Wolfrum (ed.), *Max Planck Encyclopedia of Public International Law* (Oxford: Oxford University Press 2013)

- Oona Hathaway et al, 'The Law of Cyber Attack', *California Law Review* 100 (2012), 817–885
- Melissa Hathaway, 'Introduction: International Engagement on Cyber V: Securing Critical Infrastructure', *Georgetown Journal of International Affairs* (2015), 3–7
- Sarah Heathcote, 'State Omissions and Due Diligence: Aspects of Fault, Damage and Contribution to Injury in the Law of State Responsibility', in Karine Bannelier/Theodore Christakis/Sarah Heathcote (eds.), *The ICJ and the Evolution of International Law: The Enduring Impact of the Corfu Channel Case* (London et al.: Routledge 2012), 295–314
- Wolf Heintschel von Heinegg, 'Legal Implications of Territorial Sovereignty in Cyberspace', in Christian Czosseck/Rain Ottis/Katharina Ziolkowski (eds.), *International Conference on Cyber Conflict* (2012), 7–19
- Caitriona Heintz, 'Recommendation para. 13i', in Eneken Tikk (ed.), *Voluntary, Non-Binding Norms for Responsible State Behaviour in the Use of Information and Communications Technology – A Commentary* (United Nations Office for Disarmament Affairs 2017), 223–239
- Kevin Jon Heller, 'In Defense of Pure Sovereignty in Cyberspace', *International Law Studies* 97 (2021), 1432–1499
- An Hertogen, 'Letting Lotus Bloom', *European Journal of International Law* 26 (2015), 901–926
- Stephen C. Hicks, 'International Order and Article 38(1)(c) of the Statute of the International Court of Justice', *Suffolk Transnational Law Journal* 2 (1978), 1–42
- Zine Homburger, 'Recommendation 13a', in Eneken Tikk (ed.) *Voluntary, Non-Binding Norms for Responsible State Behaviour in the Use of Information and Communications Technology – A Commentary*, (United Nations Office for Disarmament Affairs 2017), 9–25
- Eric Hutchins/Michael J. Cloppert/Rohan M. Amin, 'Reconnaissance, Weaponization, Delivery, Exploitation, Installation, Command and Control and Action on objective', in *Information Warfare & Security Research* 1 (2011), 1–14
- Eric Talbot Jensen, 'Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right to Self-Defense', *Stanford Journal of International Law* (38) 2002, 207–240
- Jason D. Jolley, 'Recommendation para. 13f', in Eneken Tikk (ed.), *Voluntary, Non-Binding Norms for Responsible State Behaviour in the Use of Information and Communications Technology – A Commentary* (United Nations Office for Disarmament Affairs 2017), 169–190
- Jason D. Jolley, *Attribution, State Responsibility, and the Duty to Prevent Malicious Cyber-Attacks in International Law* (University of Glasgow 2017)
- Christopher C. Joyner, 'Coercion', in Rüdiger Wolfrum (ed.), *Max Planck Encyclopedia of Public International Law* (Oxford: Oxford University Press 2006)
- Asaf Lubin, 'The Liberty to Spy', *Harvard International Law Journal* 61 (2020), 185–243
- Jörn Axel Kämmerer, 'Comity', in Rüdiger Wolfrum (ed.), *Max Planck Encyclopedia of Public International Law* (Oxford: Oxford University Press 2020)

Bibliography

- Krešimir Kamber, 'Substantive and Procedural Criminal Law Protection of Human Rights in the Law of the European Convention on Human Rights', *Human Rights Law Review* 20 (2020), 75–100
- Jörg Kammerhofer, 'Uncertainty in the Formal Sources of International Law: Customary International Law and Some of Its Problems', *European Journal of International Law* 15 (2004), 523–553
- Menno T. Kamminga, 'Extraterritoriality', in Rüdiger Wolfrum (ed.), *Max Planck Encyclopedia of Public International Law* (Oxford: Oxford University Press 2012)
- Helen Keller, 'Friendly Relations Declaration (1970)', in Anne Peters (ed.), *Max Planck Encyclopedia of Public International Law* (Oxford: Oxford University Press 2021)
- Ido Kilovaty, 'The Elephant in the Room: Coercion', *AJIL Unbound* 113 (2019), 87–91
- Frederic L. Kirgis, 'Custom on a Sliding Scale', *American Journal of International Law* 81 (1987), 146–151
- Uta Kohl, 'Jurisdiction in Cyberspace', in Nicholas Tsagourias/Russell Buchan (eds.) *Research Handbook on International Law and Cyberspace* (Cheltenham: Edward Elgar Publishing 2015), 30–54
- Jeff Kosseff, 'Collective Countermeasures in Cyberspace', in *Notre Dame Journal of International and Comparative Law* 10 (2020), 18–39
- Jan Kleijssen/Pierluigi Perri, 'Cybercrime, Evidence and Territoriality: Issues and Options', in Martin Kuijjer/Wouter Werner (eds.), *The Changing Nature of Territoriality in International Law* (Netherlands Yearbook of International Law 2016), 147–173
- Thomas Kleinlein, 'Customary International Law and General Principles Rethinking Their Relationship', in Brian D. Lepard (ed.) *Reexamining Customary International Law* (Cambridge: Cambridge University Press 2017), 131–158
- Stephen D. Krasner, *Sovereignty: Organized Hypocrisy* (Princeton: Princeton University Press 1999)
- Markus Krajewski, 'Due Diligence in International Trade Law', in Heike Krieger/Anne Peters/Leonhard Kreuzer, *Due Diligence in the International Legal Order* (Oxford: Oxford University Press 2020), 312–328
- Leonhard Kreuzer, 'Sovereignty in Cyberspace – A Rule Without Content?', in Antonio Segura Serrano (ed.), *Global Cybersecurity and International Law* (London: Routledge 2024), 29–43.
- Leonhard Kreuzer, 'Hobbesscher Naturzustand im Cyberspace? Enge Grenzen der Völkerrechtsdurchsetzung bei Cyberangriffen', in Ines-Jacqueline Werkner/Niklas Schörnig (eds.), *Cyberwar – die Digitalisierung der Kriegsführung* (Wiesbaden: Springer 2019), 63–86
- Heike Krieger/Jonas Püschmann, 'Law-making and legitimacy in international humanitarian law', in Heike Krieger (ed.), *Law-Making and Legitimacy in International Humanitarian Law* (Cheltenham et al.: Edward Elgar 2021), 1–14
- Heike Krieger/Anne Peters, 'Due Diligence and Structural Change in the International Legal Order', in Heike Krieger/Anne Peters/Leonhard Kreuzer, *Due Diligence in the International Legal Order* (Oxford: Oxford University Press 2020), 351–390

- Heike Krieger, 'Conceptualizing Cyberwar, Changing the Law by Imagining Extreme Conditions?', in Thomas Eger/Stefan Oeter/Stefan Voigt (eds), *International Law and the Rule of Law under Extreme Conditions: An Economic Perspective* (Tübingen: Mohr Siebeck 2017), 195–212
- Heike Krieger/Georg Nolte, 'The International Rule of Law – Rise or Decline? – Approaching Current Foundational Challenges', in Heike Krieger/Georg Nolte/Andreas Zimmermann (eds.), *The International Rule of Law: Rise or Decline?* (Oxford: Oxford University Press 2019), 3–30.
- Heike Krieger/Anne Peters/Leonhard Kreuzer, *Due Diligence in the International Legal Order* (Oxford: Oxford University Press 2020)
- Heike Krieger, 'Positive Verpflichtungen unter der EMRK: Unentbehrliches Element einer gemeineuropäischen Grundrechtsdogmatik, leeres Versprechen oder Grenze der Justiziabilität?', *Zeitschrift für ausländisches öffentliches Recht und Völkerrecht* 74 (2014), 187–213
- Heike Krieger, 'Krieg gegen anonymous', *Archiv des Völkerrechts* 50 (2012), 1–20
- Philip Kunig, 'Prohibition of Intervention', in Rüdiger Wolfrum (ed.), *Max Planck Encyclopedia of Public International Law* (Oxford: Oxford University Press 2008)
- Henning Christian Lahmann, 'On the Politics and Ideologies of the Sovereignty Discourse in Cyberspace', *Duke Journal of Comparative & International Law* 32 (2021), 61–107
- Henning Christian Lahmann, *Unilateral Remedies to Cyber Operations: Self-Defence, Countermeasures, Necessity, and the Question of Attribution* (Cambridge: Cambridge University Press 2020)
- Henning Lahmann/Robin Geiß, 'Freedom and Security in Cyberspace: Non-Forcible Countermeasures and Collective Threat-Prevention', in Katharina Ziolkowski (ed.) *Peacetime Regime for State Activities in Cyberspace* (NATO CCDCOE 2013), 621–657
- Laurens Lavrysen, *Human Rights in a Positive State* (Cambridge et al.: intersentia 2017)
- Brian Leppard (ed.), *Re-examining Customary International Law* (Cambridge: Cambridge University Press, 2016)
- Martin C. Libicki, 'Cyberspace is not a Warfighting Domain', *I/S: A Journal of Law and Policy for the Information Society* 8 (2012), 321–336
- Andreas Lichter/Max Löffler/Sebastian Sieglöck, 'The Long-Term Costs of Government Surveillance', *Journal of the European Economic Association* 19 (2021), 741–789
- Kubo Mačák, 'From Cyber Norms to Cyber Rules: Re-engaging States as Law-makers', *Leiden Journal of International Law* 30 (2017), 877–899
- Ian H. Mack, *Towards Intelligent Self-Defence: Bringing Peacetime Espionage in From the Cold and Under the Rubric of the Right of Self-Defence* (Sydney Law School 2013)
- Dieter Martiny, 'Mutual Legal Assistance in Civil and Commercial Matters', in Rüdiger Wolfrum (ed.), *Max Planck Encyclopedia of Public International Law* (Oxford: Oxford University Press 2009)
- Nele Matz-Lück, 'Norm Interpretation across International Regimes: Competences and Legitimacy', in Margaret A. Young (ed.), *Regime Interaction in International Law – Facing Fragmentation* (Cambridge: Cambridge University Press 2012), 201–234

- Barrie Sander, 'Democracy Under The Influence: Paradigms of State Responsibility for Cyber Influence Operations on Elections', *Chinese Journal of International Law* 18 (2019), 1–56
- Beth van Schaack, 'The United States' Position on the Extraterritorial Application of Human Rights Obligations: Now is the Time for Change', *International Law Studies* 90 (2014), 20–65
- Oscar Schachter, *International Law in Theory and Practice* (Dordrecht et al.: Martinus Nijhoff 1991)
- Stein Schjolberg/Solange Ghernaouti-Hélie, *A Global Treaty on Cybersecurity and Cybercrime* (2nd edition, Oslo: AiTOslo 2011)
- Michael N. Schmitt (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge: Cambridge University Press 2017)
- Michael N. Schmitt/Liis Vihul, 'Respect for Sovereignty in Cyberspace', *Texas Law Review* 95 (2017), 1639–1670
- Michael N. Schmitt, 'In Defense of Due Diligence in Cyberspace', *Yale Law Journal Forum* 125 (2015), 68–81
- Sven-Hendrik Schulze, *Cyber-»War« – Testfall der Staatenverantwortlichkeit* (Tübingen: Mohr Siebeck 2015)
- Antonio Segura-Serrano, 'The Challenge of Global Cybersecurity', in: Antonio Segura-Serrano (ed.), *Global Cybersecurity and International Law* (Routledge 2024), 1–9
- Anja Seibert-Fohr, 'From Complicity to Due Diligence: When Do States Incur Responsibility for Their Involvement in Serious International Wrongdoing?', *German Yearbook of International Law* 60 (2017), 667–708
- Yuval Shany, 'Taking Universality Seriously: A Functional Approach to Extraterritoriality in International Human Rights Law', *The Law & Ethics of Human Rights* 7 (2013), 47–71
- Dinah L. Shelton, 'Law, Non-Law and the Problem of "Soft Law"', in Dina L. Shelton (ed.) *Commitment and Compliance: The Role of Non-Binding Norms in the International Legal System* (Oxford: Oxford University Press 2000), 1–20
- Christina Parajon Skinner, 'An International Law Response to Economic Cyber Espionage', *Connecticut Law Review* 46 (2014) 1165–1207
- Matthew Sklerov, 'Solving the Dilemma of State Response to Cyberattacks', *Military Law Review* 201 (2009), 1–85
- Peter Stockburger, 'From Grey Zone to Customary International Law: How Adopting the Precautionary Principle May Help Crystallize the Due Diligence Principle in Cyberspace', in Tomáš Minárik/Raik Jakschis/Lauri Lindström (eds.), *10th International Conference on Cyber Conflict CyCon X: Maximising Effects 2018* (NATO CCD COE 2018), 245–262
- Vladislava Stoyanova, 'Fault, Knowledge and Risk Within the Framework of Positive Obligations under the European Convention on Human Rights', *Leiden Journal of International Law* 33 (2020), 601–620
- Jamie Strawbridge, 'The Big Bluff: Obama, Cyber Economic Espionage, and the Threat of WTO Litigation', *Georgetown Journal of International Law* 47 (2016), 833–870

- Milan Tahraoui, 'Surveillance des flux de données: juridiction ou compétences de l'État, des notions à refonder', in Matthias Audit/Etienne Pataut (eds.), *Lextraterritorialité* (Paris: Pedone 2020), 141–194
- Stefan Talmon, 'Determining Customary International Law: The ICJ's Methodology between Induction, Deduction and Assertion', *European Journal of International Law* 26 (2015), 417–443
- Christian Tams, *Enforcing Obligations Erga Omnes in International Law* (Cambridge University Press 2009)
- Attila Tanzi, 'Liability for Lawful Acts', in Rüdiger Wolfrum (ed.), *Max Planck Encyclopedia of Public International Law* (Oxford: Oxford University Press 2010)
- Hugh W.A Thirlway, *International Customary Law and Codification: An Examination of the Continuing Role of Custom in the Present Period of Codification of International Law* (Leiden: Sijthoff 1972)
- Eneken Tikk, 'Introduction', in Eneken Tikk (ed.), *Voluntary, Non-Binding Norms for Responsible State Behaviour in the Use of Information and Communications Technology – A Commentary* (United Nations Office for Disarmament Affairs 2017)
- Eneken Tikk/Kadri Kaska/Liis Vihul, *International Cyber Incidents – Legal Considerations* (NATO CCDCOE 2010)
- Stephen Townley, 'The Rise of Risk in International Law', *Chicago Journal of International Law* 18 (2018), 594–646
- Arie Trouwborst, *Precautionary Rights and Duties of States* (Leiden/Boston: Martinus Nijhoff 2006)
- Nicholas Tsagourias/Michael Farrell, 'Cyber Attribution: Technical and Legal Approaches and Challenges', *European Journal of International Law* 31 (2020), 941–967
- Nicholas Tsagourias, 'Recommendation 13j', in Eneken Tikk (ed.), *Voluntary, Non-Binding Norms for Responsible State Behaviour in the Use of Information and Communications Technology – A Commentary* (United Nations Office for Disarmament Affairs 2017), 241–264
- Bobby Vedral, 'The Vulnerability of the Financial System to a Systemic Cyberattack', in Taťána Jančárková/Lauri Lindström et al. (eds.), *Going Viral* (NATO CCDCOE 2021), 95–110
- Eleonora Viganò/Michele Loi/Emad Yaghmaei, 'Cybersecurity of Critical Infrastructure', in Markus Christen Bert Gordijn Michele Loi (eds.), *The Ethics of Cybersecurity* (Berlin: Springer Nature 2020), 157–178
- Federica Violi, 'The Function of the Triad "Territory", "Jurisdiction", and "Control" in Due Diligence Obligations', in Heike Krieger/Anne Peters/Leonhard Kreuzer, *Due Diligence in the International Legal Order* (Oxford: Oxford University Press 2020), 75–91
- Silja Vöneky, 'Analogy', in Anne Peters (ed.), *Max Planck Encyclopedia for Public International Law* (Oxford: Oxford University Press 2020)
- Beatrice A. Walton, 'Duties Owed: Low-Intensity Cyber Attacks and Liability for Transboundary Torts in International Law', *Yale Law Journal* 126 (2017), 1460–1519

Bibliography

- Sean Watts, 'Low-Intensity Cyber Operations and the Principle of Non-Intervention,' in Jens D. Ohlin/Kevin Govern/Claire Finkelstein, *Cyber War: Law and Ethics for Virtual Conflicts* (Oxford: Oxford University Press 2015), 249–270
- Stephan Wilske, 'Abduction', in Rüdiger Wolfrum (ed.), *Max Planck Encyclopedia of Public International Law* (Oxford: Oxford University Press 2019)
- Thomas Wischmeyer, *Informationssicherheit* (Tübingen: Mohr Siebeck 2023)
- Rüdiger Wolfrum/Mirka Möldner, 'International Courts and Tribunals, Evidence', in Rüdiger Wolfrum (ed.), *Max Planck Encyclopedia of Public International Law* (Oxford: Oxford University Press 2013)
- Rüdiger Wolfrum, 'International Law of Cooperation', in Rüdiger Wolfrum (ed.), *Max Planck Encyclopedia of Public International Law* (Oxford: Oxford University Press 2010)
- Johann-Christoph Woltag, *Cyber Warfare: Military Cross-Border Computer Network Operations Under International Law* (Cambridge et al.: Intersentia 2014)
- Michael Wood, 'Customary International Law and the General Principles of Law Recognized by Civilized Nations', *International Community Law Review* 21 (2019) 307–324
- William Thomas Worster, 'The Inductive and Deductive Methods in Customary International Law Analysis: Traditional and Modern Approaches', *Georgetown Journal of International Law* 45 (2014), 445–521
- Quincy Wright, 'Espionage and the Doctrine of Non-Intervention in Internal Affairs', in Roland J. Stanger (ed.), *Essays on Espionage and International Law* (Columbus: Ohio State University Press 1962)
- Li Zhang, 'A Chinese Perspective on Cyber War', *International Review of the Red Cross* 94 (2012), 801–807
- Zhixiong Huang/Kubo Mačák, 'Towards the International Rule of Law in Cyberspace: Contrasting Chinese and Western Approaches', *Chinese Journal of International Law* 16 (2017), 271–310
- Katharina Ziolkowski, 'General Principles of International Law as Applicable in Cyberspace' in Katharina Ziolkowski (ed.) *Peacetime Regime for State Activities in Cyberspace* (NATO CCDCOE 2013), 135–188

Blogposts

- Dapo Akande/Antonio Coco/Talita de Souza Dias, 'Old Habits Die Hard: Applying Existing International Law in Cyberspace and Beyond', 5 January 2021, *EJIL:Talk!*, available at: <https://www.ejiltalk.org/old-habits-die-hard-applying-existing-international-law-in-cyberspace-and-beyond/>
- Prableen Bajpai, 'The 5 Largest Economies In The World And Their Growth In 2020', *Nasdaq*, 22 January 2020, available at: <https://www.nasdaq.com/articles/the-5-largest-economies-in-the-world-and-their-growth-in-2020-2020-01-22>
- Russell Buchan, 'Eye on the Spy: International Law, Digital Supply Chains and the SolarWinds and Microsoft Hacks', *Völkerrechtsblog*, 31 March 2021, available at: <https://voelkerrechtsblog.org/de/eye-on-the-spy/>

- Gary Corn, 'Covert Deception, Strategic Fraud, and the Rule of Prohibited Intervention', *LawfareBlog*, 24 September 2020, available at: <https://www.lawfareblog.com/covert-deception-strategic-fraud-and-rule-prohibited-intervention>
- Kristen Eichensehr, 'Three Questions on the WannaCry Attribution to North Korea', *JustSecurity*, 20 December 2017, available at: <https://www.justsecurity.org/49889/questions-wannacry-attribution-north-korea>
- Tomaso Falchetta, 'The Draft UN Cybercrime Treaty Is Overbroad and Falls Short On Human Rights Protection', *JustSecurity*, 22 January 2024, available at: <https://www.justsecurity.org/91318/the-draft-un-cybercrime-treaty-is-overbroad-and-falls-short-on-human-rights-protection/>
- Michael P. Fischerkeller, 'Current International Law Is Not an Adequate Regime for Cyberspace', *LawfareBlog*, 22 April 2021, available at: <https://www.lawfareblog.com/current-international-law-not-adequate-regime-cyberspace>
- Jack Goldsmith, 'Self-Delusion on the Russia Hack', 18 December 2020, *The Dispatch*, available at: <https://thedispatch.com/p/self-delusion-on-the-russia-hack?s=r>
- Oona Hathaway/Alasdair Phillips-Robins, 'COVID-19 and International Law Series: Vaccine Theft, Disinformation, the Law Governing Cyber Operations', *JustSecurity*, 4 December 2020, available at: <https://www.justsecurity.org/73699/covid-19-and-international-law-series-vaccine-theft-disinformation-the-law-governing-cyber-operations/>
- Sven Herpig/Ari Schwartz, 'The Future of Vulnerabilities Equities Processes Around the World', *Lawfare*, 4 January 2019, available at: <https://www.lawfareblog.com/future-vulnerabilities-equities-processes-around-world>
- Leonhard Kreuzer, 'Disentangling the Cyber Security Debate', *Völkerrechtsblog*, 20 June 2018, available at: <https://voelkerrechtsblog.org/de/disentangling-the-cyber-security-debate/>
- Heike Krieger, 'Sovereignty – an Empty Vessel?', *EJIL:Talk!*, 7 July 2020, available at: <https://www.ejiltalk.org/sovereignty-an-empty-vessel/>
- Marko Milanovic, 'Wieder and Guarneri v UK: A Justifiably Expansive Approach to the Extraterritorial Application of the Right to Privacy in Surveillance Cases', *EJIL:Talk!*, 21 March 2024, available at: <https://www.ejiltalk.org/wieder-and-guarneri-v-uk-a-justifiably-expansive-approach-to-the-extraterritorial-application-of-the-right-to-privacy-in-surveillance-cases/>
- Marko Milanovic, 'The Grand Normalization of Mass Surveillance: ECtHR Grand Chamber Judgments in Big Brother Watch and Centrum för rättvisa', *EJIL:Talk!*, 26 May 2021 available at: <https://www.ejiltalk.org/the-grand-normalization-of-mass-surveillance-ecthr-grand-chamber-judgments-in-big-brother-watch-and-centrum-for-rattvisa/>
- Anne Peters, 'Surveillance Without Borders? The Unlawfulness of the NSA-Panopticon, Part II', *EJIL:Talk!*, 4 November 2013, available at: <https://www.ejiltalk.org/surveillance-without-borders-the-unlawfulness-of-the-nsa-panopticon-part-ii/>
- Mark Pomerleau, 'What is 'sovereignty' in cyberspace? Depends who you ask', *FifthDomain*, 21 November 2019, available at: <https://www.c4isrnet.com/international/2019/11/21/what-is-sovereignty-in-cyberspace-depends-who-you-ask/>

Bibliography

- Przemysław Roguski, 'The Importance of New Statements on Sovereignty in Cyberspace by Austria, the Czech Republic and United States', 11 May 2020, *JustSecurity*, available at: <https://www.justsecurity.org/70108/the-importance-of-new-statements-on-sovereignty-in-cyberspace-by-austria-the-czech-republic-and-united-states/>
- Michael N. Schmitt, 'Three International Law Rules for Responding Effectively to Hostile Cyber Operations', *JustSecurity*, 13 July 2021, available at: <https://www.justsecurity.org/77402/three-international-law-rules-for-responding-effectively-to-hostile-cyber-operations/>
- Michael N. Schmitt, 'The Sixth United Nations GGE and International Law in Cyberspace', *JustSecurity*, 10 June 2021, available at: <https://www.justsecurity.org/76864/the-sixth-united-nations-gge-and-international-law-in-cyberspace/>
- Michael N. Schmitt, 'Terminological Precision and International Cyber Law', *Articles of War*, 29 July 2021, available at: <https://lieber.westpoint.edu/terminological-precision-on-international-cyber-law/>
- Michael N. Schmitt, 'Russia's SolarWinds Operation and International Law', *JustSecurity*, 21 December 2020, available at: <https://www.justsecurity.org/73946/russias-solar-winds-operation-and-international-law/>
- Michael N. Schmitt, 'In Defense of Sovereignty in Cyberspace', *JustSecurity*, 8 May 2018, available at: <https://www.justsecurity.org/55876/defense-sovereignty-cyberspace/>
- Alexis Steffaro, 'Detour or Deadlock? Decoding the Suspended UN Cybercrime Treaty Negotiations', 4 March 2024, available at: <https://www.centerforcybersecuritypolicy.org/insights-and-research/detour-or-deadlock-decoding-the-suspended-un-cybercrime-treaty-negotiations/>
- Yevgeny Vindman, 'Is the SolarWinds Cyberattack an Act of War? It Is, If the United States Says It Is', *JustSecurity*, available at: <https://www.lawfareblog.com/solarwinds-cyberattack-act-war-it-if-united-states-says-it/>

Research paper

- Annegret Bendiek, 'Due Diligence in Cyberspace – Guidelines for International and European Cyber Policy and Cybersecurity Policy', *Stiftung Wissenschaft und Politik – Research Paper* 2016
- Carme Colomina/Héctor Sanchez Margalef/Richard Youngs, 'The Impact of Disinformation on Democratic Processes and Human Rights in the World', *Study Requested by the DROI subcommittee* (European Parliament), April 2021
- David P. Fidler, 'Economic Cyber Espionage and International Law: Controversies Involving Government Acquisition of Trade Secrets Through Cyber Technologies', *ASIL Insights* 17 (2013)
- Sven Herpig, *Active Cyber Defense – Toward Operational Norms* (Stiftung Neue Verantwortung 2023)
- Sven Herpig, *A Framework for Government Hacking in Criminal Investigations* (Stiftung Neue Verantwortung 2018)

- Klaus Lenssen, '...on the Ground: An Industry Perspective', in Ingolf Pernice/Jörg Pohle (eds.), *Privacy and Cyber Security on the Books and on the Ground* (Alexander von Humboldt Institute for Internet and Society 2018), 107–110
- James Lewis, 'Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats', Center for Strategic and International Studies 2002
- Tambiana Madiaga, 'Digital Sovereignty for Europe', *EPRS – European Parliamentary Research Service*, July 2020
- Zhanna Malekos Smith/Eugenia Lostri/James A. Lewis (Project Director), McAfee, 'The Hidden Costs of Cybercrime', 9 December 2020
- Tim Maurer/Robert Morgus, *Tipping the Scale: An Analysis of Global Swing States in the Internet Governance Debate* (The Centre for International Governance Innovation and the Royal Institute for International Affairs 2014)
- Harriet Moynihan, 'The Application of International Law to State Cyberattacks Sovereignty and Non-intervention', *Chatham House – Research Paper*, 2019
- Przemysław Roguski, 'Application of International Law to Cyber Operations: A Comparative Analysis of States' Views', *The Hague Program for Cyber Norms, Policy Brief*, 2020
- Christina Rupp/Alexandra Paulus, *Official Public Political Attribution of Cyber Operations – State of Play and Policy Options* (Stiftung Neue Verantwortung 2023)
- Stefan Talmon, 'Das Abhören des Kanzlerhandys und das Völkerrecht', *Bonn Research Papers on Public International Law* 3 (2013)
- Eneken Tikk/Mika Kerttunen, 'The Alleged Demise of the UN GGE: An Autopsy and Eulogy', *Cyber Policy Institute*, 2017
- Ann Valjataga, 'Tracing Opinio Juris in National Cyber Security Strategy Documents', *NATO CCDCOE 2018*, 1–18
- Expert testimonies
- Helmut Philipp Aust, 1. Untersuchungsausschuss der 18. Wahlperiode des Deutschen Bundestages Stellungnahme zur Sachverständigenanhörung am 5. Juni 2014
- Non-legal articles/news (online)*
- Ronen Bergman/David M Halbfinger, 'Israel Hack of Iran Port Is Latest Salvo in Exchange of Cyberattacks', *NYTimes*, 18 May 2021
- Ronen Bergman/Rick Gladstone/Farnaz Fassihi, 'Blackout Hits Iran Nuclear Site in What Appears to Be Israeli Sabotage', *New York Times*, 11 April 2021
- Patrick Beuth, 'Der Spionagefall des Jahres', *Der Spiegel*, 18 December 2020
- Russell Brandom, 'UK Hospitals Hit with Massive Ransomware Attack', *The Verge*, 12 May 2017, available at: <https://www.theverge.com/2017/5/12/15630354/nhs-hospitals-ransomware-hack-wannacry-bitcoin>
- Gary D. Brown/Owen W. Tullos, 'On the Spectrum of Cyberspace Operations', *Small Wars Journal*, 11 December 2012, available at: <https://smallwarsjournal.com/jrnl/art/on-the-spectrum-of-cyberspace-operations>
- Kellen Browning, 'Hundreds of Businesses, From Sweden to U.S., Affected by Cyberattack', *New York Times*, 2 July 2021

Bibliography

- Tom Burt, 'New Cyberattacks Targeting U.S. Elections', *MicrosoftBlog*, 10 September 2020
- Adrian Croft, 'EU Threatens to Suspend Data-sharing with U.S. over Spying Reports', *Reuters*, 5 July 2013, available at: <https://www.reuters.com/article/usa-security-eu-idNDEE96409F20130705>
- Grace Dobush, '20-year-old German Hacker Confesses in Doxing Case', *Handelsblatt*, 1 August 2019
- Ryan Dube, 'What Is Binary Code and How Does It Work?', *Lifewire*, 2 March 2022, available at: <https://www.lifewire.com/what-is-binary-and-how-does-it-work-4692749>
- Myriam Dunn Cavelty/Jacqueline Eggenschwiler, 'Behavioral Norms in Cyberspace', *The Security Times*, February 2019
- Melissa Eddy/Nicole Pelroth, 'Cyber Attack Suspected in German Woman's Death', *New York Times*, 18 September 2020,
- Josh Frühliner, 'The CIA Triad: Definition, Components and Examples', *CSO Online*, 10 February 2020, available at: <https://www.csoonline.com/article/3519908/the-cia-triad-definition-components-and-examples.html>
- Alex Grigsby, 'The United Nations Doubles Its Workload on Cyber Norms, and Not Everyone Is Pleased', *Council on Foreign Relations*, 15 November 2018, available at: <https://www.cfr.org/blog/united-nations-doubles-its-workload-cyber-norms-and-not-everyone-pleased>
- Thomas Holt, 'What Are Software Vulnerabilities, and Why Are There so Many of Them?', *The Conversation*, 23 May 2017
- Michael Knigge, 'NSA Surveillance Eroded Transatlantic Trust', *DW*, 27 December 2013, available at: <https://www.dw.com/en/nsa-surveillance-eroded-transatlantic-trust/a-17311216>
- Meike Laaff, 'Wie eine Cyberattacke einen ganzen Landkreis lahmlegt', *ZEIT Online*, 12 July 2021
- Steve Morgan, 'Cybercrime To Cost The World \$10.5 Trillion Annually By 2025', 13 November 2020, available at: <https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/>
- Olga Pavlova, 'Putin says Russia Prepared to Extradite Cyber Criminals to US on Reciprocal Basis', *CNN*, 13 June 2021
- Chad Perrin, 'The CIA Triad', *TechRepublic*, 30 June 2008, available at: <https://www.techrepublic.com/article/the-cia-triad/>
- Ian Phillips/Vladimir Isachenkov, 'Putin: Russia Doesn't Hack but "Patriotic" Individuals Might', *APNews*, 1 June 2017
- James Risen/Eric Lichtblau, 'How the U.S. Uses Technology to Mine More Data More Quickly', *New York Times*, 8 June 2013
- Irina Rizmal, 'Cyberterrorism: What Are We (not) Talking About?', *Diplo*, 3 August 2017
- Jordan Robertson/Laurence Arnold, 'Cyberwar: How Nations Attack Without Bullets or Bombs', *Washington Post*, 14 December 2020

- Dan Sabbagh/Andrew Roth, 'Russian State-Sponsored Hackers Target Covid-19 Vaccine Researchers', *Guardian*, 16 July 2020
- David E. Sanger/Nicole Perlroth/Eric Schmitt, 'Scope of Russian Hacking Becomes Clear: Multiple U.S. Agencies Were Hit', *New York Times*, 9 September 2021
- Bruce Schneier, 'Class Breaks', *Schneier on Security*, 3 January 2017
- Bruce Schneier, 'Simultaneous Discovery of Vulnerabilities', *Schneier on Security*, 15 February 2016
- Vladimir Soldatkin/Humeyra Pamuk, 'Biden Tells Putin Certain Cyberattacks Should be 'off-limits'', *Reuters*, 17 June 2021
- Robert Sprague/Sean Valentine, 'Due Diligence', *Encyclopædia Britannica*, 4 October 2018.
- Mehul Srivastava, 'WhatsApp voice calls used to inject Israeli spyware on phones', *Financial Times*, 14 May 2019
- Friedel Taube, 'Russia-Ukraine Conflict: What Role Do Cyberattacks Play?', *Deutsche Welle*, 28 February 2022, available at: <https://www.dw.com/en/russia-ukraine-conflict-what-role-do-cyberattacks-play/a-60945572>.
- Ian Tennant/Summer Walker, 'Cyber, Fire and Fury', *Global Initiative*, 17 March 2022, available at: <https://globalinitiative.net/analysis/un-cybercrime-treaty/>.
- Maegan Vazquez/Allie Malloy, 'Biden Will Discuss Recent Cyber Attack on Meat Producer with Putin in Geneva', *CNN*, 2 June 2021
- Kim Zetter, 'Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid', *Wired*, 3 March 2016
- Unnamed: 'Pegasus: Spyware Sold to Governments "Targets Activists"', *BBC*, 19 July 2021, available at: <https://www.bbc.com/news/technology-57881364>
- Unnamed: 'How the Dutch Foiled Russian "Cyber-attack" on OPCW', *BBC*, 4 October 2018, available at: <https://www.bbc.com/news/world-europe-45747472>

