THE HAGUE PROGRAM on International Cyber Security

Universiteit Leiden

International Cyber Security Bibliography

Adamson, Liisi & Zine Homburger (2019) "Let Them Roar: Small States as Cyber Norm Entrepreneurs." *European Foreign Affairs Review* 24 (2): 217-234.

Akoto, William (2024) "Who spies on whom? Unravelling the puzzle of state-sponsored cyber economic espionage." *Journal of Peace Research*.

Allen, Nate D.F. & Matthew La Lime (2024) "New technology, old strategy: Cyberspace and the international politics of African agency." *Journal of Strategic Studies*.

Andersen, Lise, Dennis Broeders & Raluca Csernatoni (eds.) (2024) *Emerging and Disruptive Digital Technologies: National, Regional, and Global Perspectives*. Luxembourge, Publications Office of the European Union.

Arquilla, John (2021) *Bitskrieg: The New Challenge of Cyberwarfare*, Wiley.

Ashton-Hart, Nick (2015) "Solving the International Internet Policy Coordination Problem." *Global Commission on Internet Governance, Paper Series: No. 12 – May*, Centre for International Governance Innovation (CIGI) and Chatham House.

Austin, Greg (2016) "International Legal Norms in Cyberspace: Evolution of China's National Security Motivations." In: Osula, A.-M. & Rõigas, H. (eds), *International Cyber Norms: Legal, Policy & Industry Perspectives*, Tallinn: NATO CCD COE Publications, 171-201.

Austin, Greg, Bruce McConnell & Jan Neutze (2015) *Promoting International Cyber Norms: A New Advocacy Forum - A Report from the EastWest Institute Breakthrough Group on Promoting Measures of Restraint in Cyber Armaments*, New York: The EastWest Institute.

Backman, Sarah (2020) "Conceptualizing cyber crises." *Journal of Contingencies and Crisis Management*.

Backman, Sarah (2023) "Risk vs. threat-based cybersecurity: the case of the EU." *European Security* 23 (1): 85-103.

Backman, Sarah (2023) "Normal cyber accidents." *Journal of Cyber Policy*.

Backman, Sarah & Tim Stevens (2024) "Cyber risk logics and their implications for cybersecurity." *International Affairs* 100 (6): 2441-2460.

Baker-Beall, Christopher & Gareth Mott (2021) "Understanding the European Union's Perception of the Threat of Cyberterrorism: A Discursive Analysis." *Journal of Common Market Studies*.

This bibliography was originally started and compiled by Liisi Adamson and is maintained by the team from The Hague Program on International Cyber Security (formerly The Hague Program for Cyber Norms) - please send any additions or suggestions to info@thehagueprogram.nl

Banks, William C. (2019) "The Bumpy Road to a Meaningful International Law of Cyber Attribution." *AJIL Unbound* 113: 191-196.

Bannelier-Christakis, Karine (2019) "Due Diligence: a Strategic Norm of Responsible Behaviour for the EU Cyber Diplomacy Toolbox?." Inaugural meeting of the European Cyber Diplomacy Dialogue, EU Cyber Direct, January 2019.

Baram, Gil (2024) "Cyber Diplomacy through Official Public Attribution: Paving the Way for Global Norms." *International Studies Perspectives*.

Baram, Gil (2025) "When Intelligence Agencies Publicly Attribute Offensive Cyber Operations: Illustrative Examples from the United States." *International Journal of Intelligence and CounterIntelligence*.

Barrinha, André (2024) "Cyber-diplomacy: The Emergence of a Transient Field." *The Hague Journal of Diplomacy*.

Barrinha, André & Thomas Renard (2020) "Power and diplomacy in the post-liberal cyberspace." *International Affairs* 96 (3): 749-766.

Barrinha, André & Rebecca Turner (2023) "Strategic narratives and the multilateral governance of cyberspace: The cases of European Union, Russia and India." *Contemporary Security Policy*.

Barton, April Mara (2000) "Norm Origin and Development in Cyberspace: Models of Cybernorm Evolution." *Washington University Law Quarterly* 78 (1): 59-111.

Baseley-Walker, Ben (2011) "Transparency and Confidence-Building Measures in Cyberspace: Towards Norms of Behaviour." In: Vignard, K., McCrae, R. & Powers, J. (eds), *Disarmament Forum: Confronting Cyberconflict*, Geneva: UNIDIR, 2011 (4): 31-40.

Bates, Alicia (2022) "Prepare and Prevent: Don't Repair and Repent: The Role of Insurance in Offensive Cyber." *The Cyber Defense Review* 7 (3): 17-29.

Beaumier, Guillaume & Madison Cartwright (2024) "Cross-Network Weaponization in the Semiconductor Supply Chain." *International Studies Quarterly* 68 (1).

Bellovin, Steven M., Susan Landau & Herbert S. Lin (2017) "Limiting the undesired impact of cyber weapons: technical requirements and policy implications." *Journal of Cybersecurity* 3 (1): 59-68.

Benkler, Yochai (2000) "From Consumers to Users: Shifting the Deeper Structures of Regulation Toward Sustainable Commons and User Access." *Federal Communications Law Journal* 52 (3): 561-579.

Benson, Bruce L. (2005) "The Spontaneous Evolution of Cyber Law: Norms, Property Rights, Contracting, Dispute Resolution and Enforcement without the State." *Journal of Law, Economics & Policy* 1 (2): 269-348.

Biller, Jeffrey T. & Michael N. Schmitt (2019) "Classification of Cyber Capabilities and Operations as Weapons, Means or Methods of Warfare." *International Law Studies* 95: 179-225.

Bjola, Corneliu & Markus Kornprobst (eds) (2023) *Digital International Relations: Technology, Agency and Order*. Routledge.

Blancato, Filippo Gualtiero & Madeline Carr (2024) "The trust deficit. EU bargaining for access and control over cloud infrastructures." *Journal of European Public Policy*.

Boeke, Sergei & Dennis Broeders (2018) "The Demilitarisation of Cyber Conflict." *Survival* 60 (6): 73-90.

Boeken, Jasmijn (2024) "In Between Digital War and Peace." *Journal of Military Ethics*.

Boer, Lianne (2021) *International Law As We Know It: Cyberwar Discourse and the Construction of Knowledge in International Legal Scholarship*, Cambridge University Press.

Borghard, Erica D. & Shawn W. Lonergan (2019) "Cyber Operations as Imperfect Tools of Escalation." *Strategic Studies Quarterly* 13 (3): 122-145.

Bouza García, Luis & Alvaro Oleart (2023) "Regulating Disinformation and Big Tech in the EU: A Research Agenda on the Institutional Strategies, Public Spheres and Analytical Challenges." *Journal of Common Market Studies*.

Boyko, Sergey (2016) "UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security." *International Affairs: A Russian Journal of World Politics, Diplomacy, and International Relations* 62 (5).

Bradford, Anu (2023) *Digital Empires: The Global Battle to Regulate Technology*. Oxford University Press.

Bradshaw, Samantha & Laura DeNardis (2024) "Technical infrastructure as a hidden terrain of disinformation." *Journal of Cyber Policy*.

Branch, Jordan (2020) "What's in a Name? Metaphors and Cybersecurity." *International Organization*: 1-32.

Brantly, Aaron F. (2020) "Entanglement in Cyberspace: Minding the Deterrence Gap." *Democracy and Security* 16 (3): 210-233.

Broeders, Dennis (2016) *The Public Core of the Internet, An International Agenda for Internet Governance*, Amsterdam: Amsterdam University Press.

Broeders, Dennis (2021) "Private active cyber defense and (international) cyber security – pushing the line?" *Journal of Cybersecurity* 7 (1).

Broeders, Dennis (2021) "The (im)possibilities of addressing election interference and the public core of the internet in the UN GGE and OEWG: a mid-process assessment." *Journal of Cyber Policy*.

Broeders, Dennis (2024) "Cyber intelligence and international security. Breaking the legal and diplomatic silence?" *Intelligence and National Security*.

Broeders, Dennis, Liisi Adamson & Rogier Creemers (2019) *A coalition of the unwilling? Chinese and Russian perspectives on cyberspace*, The Hague Program for Cyber Norms Policy Brief, November 2019.

Broeders, Dennis, Sergei Boeke & Ilina Georgieva (2019) *Foreign intelligence in the digital age. Navigating a state of 'unpeace'*, The Hague Program for Cyber Norms Policy Brief, September 2019.

Broeders, Dennis, Els De Busser & Patryk Pawlak (2020) *Three tales of attribution in cyberspace: Criminal law, international law and policy debates*, The Hague Program for Cyber Norms Policy Brief, April 2020.

Broeders, Dennis, Els De Busser, Fabio Cristiano & Tatiana Tropina (2022) "Revisiting past cyber operations in light of new cyber norms and interpretations of international law: inching towards lines in the sand?" *Journal of Cyber Policy*.

Brown, Gary & Keira Poellet (2012) "The Customary International Law of Cyberspace." *Strategic Studies Quarterly* 6 (3): 126-145.

Brunner, Isabella (2023) "Insurance Policies and the Attribution of Cyber Operations Under International Law: A Commentary." *NYU Journal of International Law and Politics* 55 (1): 179-192.

Buchan, Russell (2019) "Taking Care of Business: Industrial Espionage and International Law." *The Brown Journal of World Affairs* 26 (1): 143-160.

Buchanan, Ben & Fiona S. Cunningham (2020) "Preparing the Cyber Battlefield: Assessing a Novel Escalation Risk in a Sino-American Crisis." *Texas National Security Review* 3 (4): 54-81.

Burton, Joe (2018) "Cyber Security Norms in the Euro-Atlantic Region: NATO and the EU as Norm Entrepreneurs and Norm Diffusers." In: Gruszczak, A. & Frankowski, P. (eds), *Technology, Ethics and the Protocols of Modern War*, London: Routledge.

Burton, Joe (2022) "The Future of Cyber Conflict Studies: Cyber Subcultures and the Road to Interdisciplinarity." *The Cyber Defense Review* 7 (3): 103-115.

Burton, Joe & George Christou (2021) "Bridging the gap between cyberwar and cyberpeace." *International Affairs* 97 (6): 1727-1747.

Butler, Bob & Irving Lachow (2012) "Multilateral Approaches for Improving Global Security in Cyberspace." *Georgetown Journal of International Affairs*: 5-14.

Bygrave, Lee A. (2025) "The emergence of EU cybersecurity law: A tale of lemons, angst, turf, surf and grey boxes." *Computer Law & Security Review* 56 (April).

Calderaro, Andrea & Anthony J.S. Craig (2020) "Transnational governance of cybersecurity: policy challenge and global inequalities in cyber capacity building." *Third World Quarterly*.

Canfil, Justin Key (2024) "Until consensus: Introducing the International Cyber Expression dataset." *Journal of Peace Research*.

Carrapico, Helena Farrand, and George Christou (2024) "All in this Together? Communities of Practice in UK-EU Cybersecurity Relations Post-Brexit and Differentiated Re-engagement." *Journal of Common Market Studies*.

Carver, Julia (2024) "Developing digital "peripheries" for strategic advantage: Capacity building assistance and strategic competition in Africa." *Contemporary Security Policy*.

CCDCOE Law Branch Researchers, Kadri Kaska (ed) (2019) "Trends in International Law for Cyberspace." NATO Cooperative Cyber Defense Centre of Excellence (CCDCOE), May 2019.

Centre for International Governance Innovation & Royal Institute of International Affairs (2016) *A Universal Internet in a Bordered World: Research on Fragmentation, Openness and Interoperability (Research Volume One)*, Global Commission on Internet Governance, Centre for International Governance Innovation (CIGI) and Chatham House.

Chantzos, Ilias & Shireen Alam (2016) "Technological Integrity and the Role of Industry in Emerging Cyber Norms." In: Osula, A.-M. & Rõigas, H. (eds), *International Cyber Norms: Legal, Policy & Industry Perspectives*, Tallinn: NATO CCD COE Publications, 203-220.

Charney, Scott, Erin English, Aaron Kleiner, Nemanja Malisevic, Angela McKay, Jan Neutze & Paul Nicholas (2016) *From Articulation to Implementation: Enabling Progress on Cybersecurity Norms*, Microsoft Corporation.

Che Mat, Nur Ilzam, Norziana Jamil, Yunus Yusoff & Miss Laiha Mat Kiah (2024) "A systematic literature review on advanced persistent threat behaviors and its detection strategy." *Journal of Cybersecurity* 10 (1): 1-18.

Chen, Xuechen & Yifan Yang (2022) "Contesting Western and Non-Western Approaches to Global Cyber Governance beyond Westlessness." *The International Spectator* 57 (3): 1-14.

Chen, Xuechen, and Xinchuchu Gao (2024) "Norm diffusion in cyber governance: China as an emerging norm entrepreneur?" *International Affairs* 100 (6): 2419-2440.

Chenou, Jean-Marie (2021) "The contested meanings of cybersecurity: evidence from post-conflict Colombia." *Conflict, Security & Development* 21 (1): 1-19.

Chertoff, Michael & Paul Rosenzweig (2015) "A Primer on Globally Harmonizing Internet Jurisdiction and Regulations." *Global Commission on Internet Governance, Paper Series: No. 10 – March*, Centre for International Governance Innovation (CIGI) and Chatham House.

Chesney, Robert & Max Smeets (2023) *Deter, Disrupt, or Deceive: Assessing Cyber Conflict as an Intelligence Contest*, Georgetown University Press.

Choucri, Nazli (2013) "Co-Evolution of Cyberspace and International Relations: New Challenges for the Social Sciences." Prepared for World Social Science Forum (WSSF) 2013 Montreal, Canada, Cambridge, MA: MIT.

Choucri, Nazli & Gaurav Agarwal (2018) "International Law for Cyber Operations: Networks, Complexity, Transparency." (Available at SSRN: https://dx.doi.org/10.2139/ssrn.3331263).

Christou, George (2016) *Cybersecurity in the European Union: Resilience and Adaptability in Governance Policy*, Palgrave Macmillan.

Christou, George (2018) "The Challenges of Cybercrime in the European Union." *European Politics and Society* 19 (3): 355-375.

Christou, George (2019) "The Collective Securitisation of Cyberspace in the European Union." *West European Politics* 42 (2): 278-301.

Claessen, Eva (2020) "Reshaping the internet – the impact of the securitisation of internet infrastructure on approaches to internet governance: the case of Russia and the EU." *Journal of Cyber Policy*.

Clarke, Richard A. (2012) *Securing Cyberspace Through International Norms: Recommendations for Policymakers and the Private Sector*, Washington D.C: Good Harbor Security Risk Management, LLC.

Claussen, Kathleen (2018) "Beyond Norms: Using International Economic Tools to Deter Malicious State-Sponsored Cyber Activities." *Temple International & Comparative Law Journal* 32 (2): 113-125. (Available at SSRN: https://ssrn.com/abstract=3395176).

Collett, Robert (2024) "Network modelling as a tool for cyber diplomacy." *Journal of Cyber Policy* 9 (3): 377-398.

Collier, Jamie (2018) "Cyber Security Assemblages: A Framework for Understanding the Dynamic and Contested Nature of Security Provision." *Politics and Governance* 6 (2): 13-21.

Corn, Gary & Eric Talbot Jensen (2018) "The Use of Force and Cyber Countermeasures." *Temple International & Comparative Law Journal* 32 (2): 127-133. (Available at SSRN: https://ssrn.com/abstract=3190253).

Cox, Joseph (2024) *Dark Wire: The Incredible True Story of the Largest Sting Operation in History*. PublicAffairs.

Crandall, Matthew & Collin Allan (2015) "Small States and Big Ideas: Estonia's Battle for Cybersecurity Norms." *Contemporary Security Policy* 36 (2): 346-368.

Creemers, Rogier (2023) "The Chinese Conception of Cybersecurity: A Conceptual, Institutional and Regulatory Genealogy." *Journal of Contemporary China*.

Creemers, Rogier, Straton Papagianneas & Adam Knight (eds) (2023) *The Emergence of China's Smart State*. Rowman and Littlefield.

Cristiano, Fabio (2018) "From Simulations to Simulacra of War: Game Scenarios in Cyberwar Exercises." *Journal of War & Culture Studies* 11 (1): 22-37.

Cristiano, Fabio (2019) "Deterritorializing Cyber Security and Warfare in Palestine: Hackers, Sovereignty, and the National Cyberspace as Normative." *CyberOrient* 13 (1): 28-42.

Cristiano, Fabio (2020) "Israel: Cyber Warfare and Security as National Trademarks of International Legitimacy." In: Romaniuk, S.N. & Manjikian, M. (eds), *The Routledge Companion to Global Cyber-Security Strategy*, Basingstoke: Palgrave MacMillan. (Available at SSRN: https://ssrn.com/abstract=3698972).

Cristiano, Fabio (2020) "Palestine: Whose Cyber Security without Cyber Sovereignty?." In: Romaniuk, S.N. & Manjikian, M. (eds), *The Routledge Companion to Global Cyber-Security Strategy*, Basingstoke: Palgrave MacMillan. (Available at SSRN: https://ssrn.com/abstract=3700850).

Cunningham, Fiona S. (2022) "Strategic Substitution: China's Search for Coercive Leverage in the Information Age." *International Security* 47 (1): 46-92.

Datta, Ahana (2025) "Structural Volatility: how great power cyber competition undermines trust in cyberspace." *SSRN*.

Davis, II, John S., Benjamin Boudreaux, Jonathan W. Welburn, Jair Aguirre, Cordaye Ogletree, Geoffrey McGovern & Michael S. Chase (2017) *Stateless Attribution: Toward International Accountability in Cyberspace*, Research Reports, Santa Monica, CA: RAND Corporation.

Davis, John A. & Charlie Lewis (2019) "Beyond the United Nations Group of Governmental Experts." *The Cyber Defense Review*: 161- 168.

Deeks, Ashley S. (2025) *The Double Black Box: National Security, Artificial Intelligence, and the struggle for Democratic Accountability*. Oxford University Press.

Deibert, Ronald J. (2025) *Chasing Shadows: Cyber Espionage, Subversion, and the Global Fight for Democracy*. Simon & Schuster.

Delerue, François (2020) *Cyber Operations and International Law*, Cambridge University Press, Vol. 146.

Delerue, François (2021) "Covid-19 and the Cyber Pandemic: A Plea for International Law and the Rule of Sovereignty in Cyberspace." In: Jancárková, T., Lindström, L., Visky, G. & Zotz, P. (eds), *2021 13th International Conference on Cyber Conflict: Going Viral*, Tallinn: NATO CCD COE Publications.

Delerue, François & Monica Kaminska (2023) "Governing cyber crises: policy lessons from a comparative analysis." *Policy Design and Practice*.

Dellago, Matthias, Andrew C. Simpson & Daniel W. Woods (2022) "Exploit Brokers and Offensive Cyber Operations." *The Cyber Defense Review* 7 (3): 31-47.

Demchak, Chris C. & Francesca Spidalieri (eds) (2022) *The Cyber Defense Review: Special Edition - Unlearned Lessons from the First Cybered Conflict Decade, 2010-2020* 7 (1).

Devanny, Joe, Ciaran Martin & Tim Stevens (2021) "On the strategic consequences of digital espionage." *Journal of Cyber Policy*.

Devanny, Joseph, Luiz Rogério Franco Goldoni & Breno Pauli Medeiros (2020) "The 2019 Venezuelan Blackout and the consequences of cyber uncertainty." *Revista Brasileira De Estudos De Defesa* 7 (2).

Douzet, Frédérick & Aude Géry (2021) "Cyberspace is used, first and foremost, to wage wars: proliferation, security and stability in cyberspace." *Journal of Cyber Policy* 6 (1).

Douzet, Frédérick, Kevin Limonier, Selma Mihoubi & Elodie René (2021) "Mapping the spread of Russian and Chinese contents on the French-speaking African web." *Journal of Cyber Policy* 6 (1).

Dunn Cavelty, Myriam (2025) *The Politics of Cyber-Security*. Routledge.

Dunn Cavelty, Myriam & Andreas Wenger (2020) "Cyber security meets security politics: Complex technology, fragmented politics, and networked science." *Contemporary Security Policy* 41 (1): 5-32.

Dunn Cavelty, Myriam & Andreas Wenger (eds) (2022) *Cyber Security Politics: Socio-Technical Transformations and Political Fragmentation*, Routledge.

Dunn Cavelty, Myriam & Max Smeets (2023) "Regulatory cybersecurity governance in the making: the formation of ENISA and its struggle for epistemic authority." *Journal of European Public Policy*.

Dunn Cavelty, Myriam, Tobias Pulver & Max Smeets (2024) "The evolution of cyberconflict studies." *International Affairs* 100 (6): 2317-2339.

Dwyer, Andrew & Amy Ertan (2022) "Introduction: An Offensive Future?" *The Cyber Defense Review* 7 (3): 9-13.

Dwyer, Andrew & Jantje Silomon (2019) "Dangerous Gaming: Cyber-Attacks, Air-Strikes and Twitter." *E-International Relations*, 23 September 2019.

Easterbrook, Frank H. (1996) "Cyberspace and the Law of the Horse." *University of Chicago Legal Forum*, Vol. 1996, Article 7.

Eggenschwiler, Jacqueline (2019) "International Cybersecurity Norm Development: The Roles of States Post-2017." *Research in Focus*, EU Cyber Direct.

Egloff, Florian J. (2019) "Contested public attributions of cyber incidents and the role of academia." *Contemporary Security Policy*.

Egloff, Florian J. (2020) "Public attribution of cyber intrusions." *Journal of Cybersecurity* 6 (1).

Egloff, Florian J. (2022) *Semi-State Actors in Cybersecurity*, Oxford University Press.

Egloff, Florian J. & James Shires (2022) "Offensive Cyber Capabilities and State Violence: Three Logics of Integration." *Journal of Global Security Studies* 7 (1).

Egloff, Florian J. & Max Smeets (2021) "Publicly attributing cyber attacks: a framework." *Journal of Strategic Studies*.

Egloff, Florian J. & Myriam Dunn Cavelty (2021) "Attribution and Knowledge Creation Assemblages in Cybersecurity Politics." *Journal of Cybersecurity* 7 (1).

Eichensehr, Kristen E. (2015) "The Cyber-Law of Nations." *The Georgetown Law Journal* 103 (2): 317-380.

Eichensehr, Kristen (2020) "The Law & Politics of Cyberattack Attribution." *UCLA Law Review* 67.

Eichensehr, Kristen (2022) "Not Illegal: The SolarWinds Incident and International Law." *European Journal of International Law*.

Eldem, Tuba (2019) "The Governance of Turkey's Cyberspace: Between Cyber Security and Information Security." *International Journal of Public Administration*.

Elliott, David (2009) "Weighing the Case For a Convention to Limit Cyberwarfare." *Arms Control Today* 39 (9): 21-27.

Erskine, Toni & Madeline Carr (2016) "Beyond 'Quasi-Norms': The Challenges and Potential of Engaging with Norms in Cyberspace." In: Osula, A.-M. & Rõigas, H. (eds.), *International Cyber Norms: Legal, Policy & Industry Perspectives*, Tallinn: NATO CCD COE Publications, 87-109.

Fairbank, Nancy Ayer (2019) "The state of Microsoft? The role of corporations in international norm creation." *Journal of Cyber Policy* 4 (3): 380-403.

Farrand, Benjamin, Helena Carrapico & Aleksei Turobov (2024) "The new geopolitics of EU cybersecurity: security, economy and sovereignty." *International Affairs* 100 (6): 2379-2397.

Farrell, Henry (2015) "Promoting Norms for Cyberspace." *Cyber Brief*, NY: Council on Foreign Relations.

Finnemore, Martha (2011) "Cultivating International Cyber Norms." In: Lord, K.M. & Sharp, T. (eds), *America's Cyber Future: Security and Prosperity in the Information Age*, Washington D.C.: Center for a New American Security, 87-102.

Finnemore, Martha (2017) "Cybersecurity and the Concept of Norms." Carnegie Endowment for International Peace, 30 November 2017.

Finnemore, Martha & Duncan Hollis (2016) "Constructing Norms for Global Cybersecurity." *American Journal of International Law* 110 (3): 425-479.

Finnemore, Martha & Duncan B. Hollis (2019) "Beyond Naming and Shaming: Accusations and International Law in Cybersecurity." *Temple University Legal Studies Research Paper No. 2019-14*. (Available at SSRN: https://dx.doi.org/10.2139/ssrn.3347958).

Flonk, Daniëlle (2021) "Emerging illiberal norms: Russia and China as promoters of internet content control." *International Affairs* 97 (6): 1925-1944.

Flonk, Daniëlle, Markus Jachtenfuchs & Anke Obendiek (2024) "Controlling internet content in the EU: towards digital sovereignty." *Journal of European Public Policy*.

Florackis, Chris, Christodoulos Louca, Roni Michaely & Michael Weber (2023) "Cybersecurity Risk." *The Review of Financial Studies* 36 (1): 351-407.

Forsyth, James Wood (2013) "What Great Powers Make It. International Order and the Logic of Cooperation in Cyberspace." *Strategic Studies Quarterly* 7 (1): 93-113.

Forsyth, James Wood & Billy E. Pope (2014) "Structural Causes and Cyber Effects: Why International Order is Inevitable in Cyberspace." *Strategic Studies Quarterly* 8 (4): 112-128.

Fouad, Noran Shafik (2021) "The non-anthropocentric informational agents: Codes, software, and the logic of emergence in cybersecurity." *Review of International Studies*: 1-20.

François, Camille & Herb Lin (2021) "The strategic surprise of Russian information operations on social media in 2016 in the United States: mapping a blind spot." *Journal of Cyber Policy* 6 (1).

Fung, Courtney J. (2023) "China's use of rhetorical adaptation in development of a global cyber order: a case study of the norm of the protection of the public core of the internet." *Journal of Cyber Policy*.

Ganz, Abra, Martina Camellini, Emmie Hine, Claudio Novelli, Huw Roberts & Luciano Floridi (2024) "Submarine Cables and the Risks to Digital Sovereignty." *Minds and Machines* 34 (31).

Gao, Xinchuchu (2022) "An Attractive Alternative? China's Approach to Cyber Governance and Its Implications for the Western Model." *The International Spectator* 57 (3): 15-30.

Gartzke, Erik & Jon R. Lindsay (2024) *Elements of Deterrence: Strategy, Technology, and Complexity in Global Politics*. Oxford University Press.

Gechlik, Mei (2017) "Appropriate Norms of State Behavior in Cyberspace: Governance in China and Opportunities for US Businesses." Hoover Working Group on National Security, Technology, and Law, Aegis Series Paper No. 1706, 28 July 2017.

Geier, Karsten (2016) "Norms, Confidence and Capacity Building: Putting the UN Recommendations on Information and Communication Technologies in the Context of International Security Into OSCE-Action." *European Cybersecurity Journal* 2 (1).

Georgieva, Ilina (2019) "The unexpected norm-setters: Intelligence agencies in cyberspace." *Contemporary Security Policy*.

Ghernaouti-Hélie, Solange (2010) "We Need a Cyberspace Treaty: Regional and bilateral agreements are not enough." *Intermedia* 38 (3): 4-5.

Gilli, Andrea & Mauro Gilli (2019) "Why China Has Not Caught Up Yet: Military-Technological Superiority and the Limits of Imitation, Reverse Engineering, and Cyber Espionage." *International Security* 43 (3): 141-189.

Gioe, David V., Michael S. Goodman & Tim Stevens (2020) "Intelligence in the Cyber Era: Evolution or Revolution?" *Political Science Quarterly* 135 (2): 191-224.

Glennon, Michael J. (2013) "The Dark Future of International Cybersecurity Regulation." *Journal of National Security Law & Policy* 6 (2): 563-570.

Goldfarb, Avi & Jon R. Lindsay (2022) "Prediction and Judgment: Why Artificial Intelligence Increases the Importance of Humans in War." *International Security* 46 (3): 7-50.

Goldman, Emily O. (2020) "From Reaction to Action: Adopting a Competitive Posture in Cyber Diplomacy." *Texas National Security Review*, special issue on Cyber Competition.

Goldschmidt, Cassio, Melissa Dark & Hina Chaudhry (2010) "Responsibility for the Harm and Risk of Software Security Flaws." In: Dark, M.J. (ed), *Information Assurance and Security Ethics in Complex Systems: Interdisciplinary Perspectives*, Hershey PA: IGI Global, 104-131.

Goldsmith, Jack (2011) "Cybersecurity Treaties: A Skeptical View." In: Berkowitz, P. (ed), *Future Challenges in National Security and Law*, Hoover Institution Press.

Grauman, Brigid (2012) *Cyber-Security: The Vexed Question of Global Rules*, Security & Defence Agenda.

Greenberg, Andy (2019) *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*, Doubleday.

Grigsby, Alex (2017) "The End of Cyber Norms." *Survival* 59 (6): 109-122.

Hamman, Seth T., Jack Mewhirter, Richard J. Harknett, Jelena Vićić & Philip White (2020) "Deciphering Cyber Operations." *The Cyber Defense Review* 5 (1): 135-152.

Hampson, Fen Osler & Michael Sulmeyer (eds) (2017) *Getting beyond Norms: New Approaches to International Cyber Security Challenges*, Centre for International Governance Innovation.

Hansel, Mischa (2023) "Great power narratives on the challenges of cyber norm building." *Policy Design and Practice*.

Harknett, Richard J. & Max Smeets (2020) "Cyber campaigns and strategic outcomes." *Journal of Strategic Studies*.

Hassib, Bassant & James Shires (2021) "Manipulating uncertainty: cybersecurity politics in Egypt." *Journal of Cybersecurity* 7 (1).

Hassib, Bassant & James Shires (2024) "Digital recognition: cybersecurity and internet infrastructure in UAE-Israel diplomacy." *International Affairs* 100 (6): 2399-2418.

Healey, Jason (2019) "The implications of persistent (and permanent) engagement in cyberspace." *Journal of Cybersecurity* 5 (1).

Healey, Jason & Hannah Pitts (2012) "Applying International Environmental Legal Norms to Cyber Statecraft." *I/S: A Journal of Law and Policy for the Information Society* 8 (2): 356-387.

Heintschel von Heinegg, Wolff (2015) "International Law and International Information Security: A Response to Krutskikh and Streltsov." *Tallinn Paper No. 9*, Tallinn: NATO CCD COE Publications.

Henschke, Adam, Matthew Sussex & Courteney O'Connor (2020) "Countering foreign interference: election integrity lessons for liberal democracies." *Journal of Cyber Policy* 5 (2): 180-198.

Herbst, Lena & Anja P. Jakobi (2024) "Opening up or closing down? Non-state actors in UN cybersecurity governance." *Journal of Global Security Studies* 9 (3): ogae026.

Hoffman, Stacie, Dominique Lazanski & Emily Taylor (2020) "Standardising the splinternet: how China's technical standards could fragment the internet." *Journal of Cyber Policy* 5 (2): 1-26.

Hoffmeister, Frank (2023) "Strategic autonomy in the European Union's external relations law." *Common Market Law Review* 60 (3): 667-700.

Holland, H. Brian (2005) "The Failure of the Rule of Law in Cyberspace?: Reorienting the Normative Debate on Borders and Territorial Sovereignty." *The John Marshall Journal of Information Technology & Privacy Law* 24 (1): 1-34.

Hollis, Duncan B. (2017) "China and the US Strategic Construction of Cybernorms: The Process is the Product." Hoover Working Group on National Security, Technology, and Law, Aegis Paper Series No. 1704, 7 July 2017.

Hollis, Duncan B., Tsvetelina J. van Benthem & Talita Dias (2022) "Information Operations under International Law." *Vanderbilt Journal of Transnational Law* 55 / Temple University Legal Studies Research Paper No. 2022-16.

Homburger, Zine (2019) "Conceptual Ambiguity of International Norms on State Behaviour in Cyberspace." *Research in Focus*, EU Cyber Direct.

Homburger, Zine (2019) "The Necessity and Pitfall of Cybersecurity Capacity Building for Norm Development in Cyberspace." *Global Society*.

Hughes, Rex (2009) "Towards a Global Regime for Cyber Warfare." In: Czosseck, C. & Geers, K. (eds), *The Virtual Battlefield: Perspectives on Cyber Warfare*, Conference proceedings - Cooperative Cyber Defense Centre of Excellence (CCD CoE) Conference on Cyber Warfare (June 2009, Tallinn, Estonia).

Hughes, Rex (2010) "A Treaty for Cyberspace." *International Affairs* 86 (2): 523-541.

Hunter, Cameron & Bleddyn E. Bowen (2023) "We'll never have a model of an AI major-general: Artificial Intelligence, command decisions, and kitsch visions of war." *Journal of Strategic Studies*.

Hurel, Louise Marie (2022) "Beyond the Great Powers: Challenges for Understanding Cyber Operations in Latin America." *Global Security Review* 2: article 7.

Hurel, Louise Marie (2022) "Interrogating the Cybersecurity Development Agenda: A Critical Reflection." *The International Spectator* 57 (3): 66-84.

Hurel, Louise Marie & Luisa Cruz Lobato (2018) "Unpacking Cyber Norms: Private Companies as Norm Entrepreneurs." *Journal of Cyber Policy* 3 (1): 61-76.

Hurwitz, Roger (2012) *An Augmented Summary of The Harvard, MIT and University of Toronto Cyber Norms Workshop*.

Hurwitz, Roger (2012) "Depleted Trust in the Cyber Commons." *Strategic Studies Quarterly* 6 (3): 20-45.

Hurwitz, Roger (2013) "A New Normal? The Cultivation of Global Norms as Part of a Cybersecurity Strategy." In: Yannakogeorgos, P.A. & Lowther, A.B. (eds), *Conflict and Cooperation In Cyberspace, The Challenge to National Security*, Taylor & Francis.

Hurwitz, Roger (2014) "The Play of States: Norms and Security in Cyberspace." *American Foreign Policy Interests: The Journal of the National Committee on American Foreign Policy* 36 (5): 322-331.

Hurwitz, Roger (2015) *A Call to Cyber Norms: Discussions at the Harvard-MIT-University of Toronto Cyber Norms Workshops, 2011 and 2012*, Belfer Center for Science and International Affairs, Kennedy School of Government, Harvard University.

Ifeanyi-Ajufo, Nnenna (2023) "Cyber governance in Africa: at the crossroads of politics, sovereignty and cooperation." *Policy Design and Practice*.

Information Technology Industry Council (2011) *The IT Industry's Cybersecurity Principles for Industry and Government*.

Inglis, John C. "Chris" (2020) "Shining a Light on Cyber: An Interview with John C. 'Chris' Inglis." *Strategic Studies Quarterly* 14 (3), 3-11.

International Security Advisory Board (ISAB) (2014) *Report on A Framework for International Cyber Stability*.

International Telecommunications Union (2014) *The Quest for Cyber Confidence*.

Ivan, Paul (2019) "Responding to cyberattacks: Prospects for the EU Cyber Diplomacy Toolbox." Europe in the World Programme Discussion Paper, European Policy Centre.

Jacobsen, Jeppe T. (2024) "Commitment and compromise in Danish cyber and tech diplomacy." *International Affairs* 100 (6): 2361-2378.

Jansen, Bernardus, Natalia Kadenko, Dennis Broeders, Michel van Eeten, Kevin Borgolte & Tobias Fiebig (2023) "Pushing boundaries: An empirical view on the digital sovereignty of six governments in the midst of geopolitical tensions." *Government Information Quarterly* 40 (4).

Johnson, David R. & David Post (1996) "Law and Borders – the Rise of Law in Cyberspace." *First Monday* 1 (1).

Johnstone, Ian, Arun Sukumar & Joel Trachtman (eds) (2023) *Building an International Cybersecurity Regime: Multistakeholder Diplomacy*. Edward Elgar.

Kadlecová, Lucie (2024) *Cyber Sovereignty: The Future of Governance in Cyberspace*. Stanford University Press.

Kadlecová, Lucie, and Viktor Paggio (2025) "Russia's Weak Spots in Cyber Sovereignty: How the West Can Keep Russian Citizens' Access to Online Information Free from the Kremlin Interference." *Democracy and Security*.

Kaljurand, Marina (2016) "United Nations Group of Governmental Experts: The Estonian Perspective." In: Osula, A.-M. & Rõigas, H. (eds), *International Cyber Norms: Legal, Policy & Industry Perspectives*, Tallinn: NATO CCD COE Publications, 111-127.

Kaminska, Monica (2021) "Restraint under conditions of uncertainty: Why the United States tolerates cyberattacks." *Journal of Cybersecurity* 7 (1).

Kania, Elsa B. (2021) "China's quest for quantum advantage – Strategic and defense innovation at a new frontier." *Journal of Strategic Studies* 44 (3): 922-952.

Kanuck, Sean (2010) "Sovereign Discourse on Cyber Conflict Under International Law." *Texas Law Review* 88 (7): 1571-1598.

Kargar, Simin & Thomas Rid (2024) "Attributing Digital Covert Action: the curious case of WikiSaudileaks." *Intelligence and National Security*.

Katagiri, Nori (2022) "Three Conditions for Cyber Countermeasures: Opportunities and Challenges of Active-Defense Operations." *The Cyber Defense Review* 7 (3): 79-89.

Katagiri, Nori (2024) "Between cyber retaliation and escalation: Explaining the variations in state compliance with the principle of proportionality." *Politics & Policy*.

Kavanagh, Camino (2012) "Cyber Dialogue 2012 Briefs: Whither "Rules of the Road" for Cyberspace?." *CyberDialogue 2012: What is Stewardship in Cyberspace*.

Keller, Kevin Jon (2021) "In Defense of Pure Sovereignty in Cyberspace." *International Law Studies* 97 (1): 1432-1499.

Kello, Lucas (2021) "Cyber legalism: why it fails and what to do about it." *Journal of Cybersecurity* 7 (1).

Kello, Lucas (2022) *Striking Back: The End of Peace in Cyberspace – And How to Restore It*, Yale University Press.

Kerttunen, Mika (2016) "Patterns of Behavior: States In, Through, and About Cyberspace." Cyber Policy Institute.

Kilovaty, Ido (2020) "Privatized Cybersecurity Law." *UC Irvine Law Review* 10 (4).

Kim, Saeme (2022) "Roles and Limitations of Middle Powers in Shaping Global Cyber Governance." *The International Spectator* 57 (3): 31-47.

Klimburg, Alexander (2020) "Mixed Signals: A Flawed Approach to Cyber Deterrence." *Survival* 62 (1): 107-130.

Klimburg, Alexander & Virgilio F.A. Almeida (2019) "Cyber Peace and Cyber Stability: Taking the Norm Road to Stability." *IEEE Internet Computing* 23 (4): 61-66.

Klimburg, Alexander & Heli Tirmaa-Klaar (2011) "Cybersecurity and Cyberpower: Concepts, Conditions and Capabilities for Cooperation for Action Within the EU." Directorate-General for External Policies of the Union, Directorate B, Policy Department, European Parliament.

Kolodii, Roman (2024) "Unpacking Russia's Cyber-Incident Response." *Security Studies*.

Komov, Sergei, Sergei Korotkov & Igor Dylevski (2007) "Military Aspects of Ensuring International Information Security in the Context of Elaborating Universally Acknowledged Principles of International Law." In: Vignard, K. (ed), *Disarmament Forum: ICTs and International Security*, Geneva: UNIDIR, 2007 (3): 3.

Korzak, Elaine (2016) "The Quest for Cyber Norms." *Bulletin of the Atomic Scientists* 72 (5): 348-350.

Kostyuk, Nadiya & Carly Wayne (2021) "The Microfoundations of State Cybersecurity: Cyber Risk Perceptions and the Mass Public." *Journal of Global Security Studies* 6 (2).

Kotasthane, Pranay & Abhiram Manchi (2023) *When the Chips Are Down: A Deep Dive into a Global Crisis*. Bloomsbury India.

Kramer, Franklin D. (2012) *Achieving International Cyber Stability*, Washington D.C.: The Atlantic Council.

Krieg, Andreas (2023) *Subversion: The Strategic Weaponization of Narratives*, Georgetown University Press.

Krutskikh, Andrey V. (2007) "[On Legal and Political Foundations of Global Information Security]." (in Russian) *Mezhdunarodniye Protsessy* 1 (5): 28–37.

Krutskikh, Andrey & Anatoly A. Streltsov (2014) "International Law and the Problem of International Information Security." *International Affairs: A Russian Journal of World Politics, Diplomacy, and International Relations* 60 (6): 64-76.

Kulikova, Alexandra (2021) "Cyber norms: technical extensions and technological challenges." *Journal of Cyber Policy* 6 (3).

Kurowska, Xymena (2019) "The politics of cyber norms: Beyond norm construction towards strategic narrative contestation." *Research in Focus*, EU Cyber Direct.

Lahmann, Henning (2020) *Unilateral Remedies to Cyber Operations: Self-Defence, Countermeasures, Necessity, and the Question of Attribution*, Cambridge University Press.

Lahmann, Henning (2023) "State Behaviour in Cyberspace: Normative Development and Points of Contention." *Zeitschrift für Außen- und Sicherheitspolitik*.

Lallie, Harjinder Singh, Lynsay Shepherd, Jason R.C. Nurse, Arnau Erola, Gregory Epiphaniou, Carsten Maple & Xavier Bellekens (2021) "Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic." *Computers & Security* 105 (June).

Lambach, Daniel (2020) "The Territorialization of Cyberspace." *International Studies Review* 22 (3): 482-506.

Lambach, Daniel & Linda Monsees (2024) "Beyond sovereignty as authority: the multiplicity of European approaches to digital sovereignty." *Global Political Economy*.

Lantis, Jeffrey S. & Daniel J. Bloomberg (2018) "Changing the code? Norm contestation and US antipreneurism in cyberspace." *International Relations* 32 (2): 149-172.

Lawson, Ewan (2022) "Between Two Stools: Military and Intelligence Organizations in the Conduct of Offensive Cyber Operations." *The Cyber Defense Review* 7 (3): 67-77.

Leal, Marcelo & Paul Musgrave (2022) "Cheerleading in Cyberspace: How the American Public Judges Attribution Claims for Cyberattacks." *Foreign Policy Analysis* 18 (2).

Lee, Heajune (2023) "Public attribution in the US government: implications for diplomacy and norms in cyberspace." *Policy Design and Practice*.

Lefebvre, Joshua (2018) "Cracking Attribution: Moving International Norms Forward." (Available at SSRN: https://dx.doi.org/10.2139/ssrn.3300202).

Leins, Kobi (2022) *New War Technologies and International Law: The Legal Limits to Weaponising Nanomaterials*, Cambridge University Press.

Lemnitzer, Jan Martin (2021) "Why cybersecurity insurance should be regulated and compulsory." *Journal of Cyber Policy*.

Lemnitzer, Jan Martin (2022) "Back to the Roots: The Laws of Neutrality and the Future of Due Diligence in Cyberspace." *European Journal of International Law* 33 (3): 789-819.

Lessig, Lawrence (1999) "The Law of the Horse: What Cyberlaw Might Teach." *Harvard Law Review* 113 (501).

Lessig, Lawrence (2006) *Code, Version 2.0*, Cambridge, MA: Basic Books.

Lewis, James A. (2010) "Multilateral Agreements to Constrain Cyberconflict." *Arms Control Today* 40 (5): 14-19.

Lewis, James Andrew (2011) "Confidence-Building and International Agreement in Cybersecurity." In: Vignard, K., McCrae, R. & Powers, J. (eds), *Disarmament Forum: Confronting Cyberconflict*, Geneva: UNIDIR, 2011 (4): 51-60.

Lewis, James Andrew (2014) "Liberty, Equality, Connectivity: Transatlantic Cybersecurity Norms." Washington D.C: Center for Strategic & International Studies.

Libicki, Martin (2017) "The Coming of Cyber Espionage Norms." In: Rõigas, H., Jakschis, R., Lindström, L. & Minárik, T. (eds), *2017 9th International Conference on Cyber Conflict: Defending the Core*, Tallinn: NATO CCD COE Publications.

Libicki, Martin C. (2018) "Expectations of Cyber Deterrence." *Strategic Studies Quarterly* 12 (4): 44-57.

Libicki, Martin C. (2020) "Norms and Normalization." *The Cyber Defense Review* 5 (1): 41-54.

Libiseller, Chiara (2023) "'Hybrid warfare' as an academic fashion." *Journal of Strategic Studies*.

Liebetrau, Tobias (2022) "Cyber conflict short of war: a European strategic vacuum." *European Security*.

Liebetrau, Tobias (2023) "Organizing cyber capability across military and intelligence entities: collaboration, separation, or centralization." *Policy Design and Practice*.

Liebetrau, Tobias (2023) "Problematising EU Cybersecurity: Exploring How the Single Market Functions as a Security Practice." *Journal of Common Market Studies*.

Liebetrau, Tobias & Linda Monsees (2024) "Cybersecurity and International Relations: developing thinking tools for digital world politics." *International Affairs* 100 (6): 2303-2315.

Lilly, Bilyana (2022) *Russian Information Warfare: Assault on Democracies in the Cyber Wild West*, Naval Institute Press.

Lin, Herbert (2016) "Attribution of malicious cyber incidents: From soup to nuts." *Journal of International Affairs* 70 (1): 75-137.

Lin, Herbert (2019) "The existential threat from cyber-enabled information warfare." *Bulletin of the Atomic Scientists* 75 (4): 187-196.

Lindsay, Jon R. (2020) "Cyber conflict vs. Cyber Command: hidden dangers in the American military solution to a large-scale intelligence problem." *Intelligence and National Security*: 1-19.

Lindsay, Jon R. (2020) *Information Technology and Military Power*, Cornell University Press.

Lindsay, Jon R. (2024) "Abducted by hackers: Using the case of Bletchley Park to construct a theory of intelligence performance that generalizes to cybersecurity." *Journal of Peace Research*.

Lonergan, Erica D. & Shawn W. Lonergan (2023) *Escalation Dynamics in Cyberspace*. Oxford University Press.

Lotrionte, Catherine (2013) "A Better Defense: Examining the United States' New Norms-Based Approach to Cyber Deterrence." *Georgetown Journal of International Affairs*: 75-88.

Lu, Chuanying (2020) "Forging Stability in Cyberspace." *Survival* 62 (2): 125-136.

Lubin, Asaf (2020) "The Liberty to Spy." *Harvard International Law Journal* 61 (1): 185.

Lubin, Asaf (2025) *The International Law of Intelligence: The World of Spycraft and the Law of Nations*. Oxford University Press.

Lucas, George (2020) "Cybersecurity and Cyber Warfare: The Ethical Paradox of 'Universal Diffidence'." In: Christen, M., Gordijn, B. & Loi, M. (eds), *The Ethics of Cybersecurity*, The International Library of Ethics, Law and Technology, 21, Springer: 245-258.

Lumiste, Liina (2022) "Russian Approaches to Regulating Use of Force in Cyberspace." *Baltic Yearbook of International Law Online* 20 (1): 109-132.

Mačák, Kubo (2015) "Military Objectives 2.0: The Case for Interpreting Computer Data as Objects under International Humanitarian Law." *Israel Law Review* 48 (1): 55-80.

Mačák, Kubo (2016) "Is the International Law of Cyber Security in Crisis?" In: Pissanidis, N., Rõigas, H. & Veenendaal, M. (eds), *2016 8th International Conference on Cyber Conflict: Cyber Power*, Tallinn: NATO CCD COE Publications, 127-139.

Mačák, Kubo (2017) "From Cyber Norms to Cyber Rules: Re-engaging States as Law-makers." *Leiden Journal of International Law* 30 (4): 877-899.

Mačák, Kubo (2021) "Unblurring the lines: military cyber operations and international law." *Journal of Cyber Policy* 6 (3).

Maschmeyer, Lennart (2021) "The Subversive Trilemma: Why Cyber Operations Fall Short of Expectations." *International Security* 46 (2).

Maschmeyer, Lennart (2023) "Subversion, cyber operations, and reverse structural power in world politics." *European Journal of International Relations* 29 (1): 79-103.

Maschmeyer, Lennart (2024) *Subversion: From Covert Operations to Cyber Conflict*. Oxford University Press.

Maschmeyer, Lennart, Alexei Abrahams, Peter Pomerantsev & Volodymyr Yermolenko (2023) "Donetsk Don't Tell – "Hybrid War" in Ukraine and the Limits of Social Media Influence Operations." *Journal of Information Technology & Politics*.

Maschmeyer, Lennart, Ronald J. Deibert & Jon R. Lindsay (2020) "A tale of two cybers-how threat reporting by cybersecurity firms systematically underrepresents threats to civil society." *Journal of Information Technology & Politics*: 1-20.

Matania, Eviatar & Udi Sommer (2023) "Tech titans, cyber commons and the war in Ukraine: An incipient shift in international relations." *International relations*.

Maurer, Tim (2011) "Cyber Norm Emergence at the United Nations, An Analysis of the UN's Activities Regarding Cyber-security." Discussion Paper 2011-11, Cambridge, Mass.: Belfer Center for Science and International Affairs, Harvard Kennedy School.

Maurer, Tim (2016) "The New Norms: Global Cyber-Security Protocols Face Challenges." *IHS Jane's Intelligence Review* March: 52-53.

Maurer, Tim (2019) "A Dose of Realism: The Contestation and Politics of Cyber Norms." *Hague Journal on the Rule of Law*: 1-23.

Maurer, Tim, Ariel (Eli) Levite & George Perkovich (2017) "Toward a Global Norm Against Manipulating the Integrity of Financial Data." Carnegie Endowment for International Peace, 27 March 2017.

Mazanec, Brian M. (2015) *The Evolution of Cyber War: International Norms for Emerging-Technology Weapons*, Lincoln, NE: University of Nebraska Press.

Mazanec, Brian M. (2015) "Why International Order in Cyberspace is Not Inevitable." *Strategic Studies Quarterly* 9 (2): 78-98.

McKay, Angela, Jan Neutze, Paul Nicholas & Kevin Sullivan (2014) *International Cybersecurity Norms: Reducing conflict in an Internet-dependent world*, Microsoft Corporation.

Melzer, Nils (2011) "Cyberwarfare and International Law." *UNIDIR Resources, Ideas for Peace and Security*.

Meyer, Paul (2020) "Norms of Responsible State Behaviour in Cyberspace." In: Christen, M., Gordijn, B. & Loi, M., *The Ethics of Cybersecurity*, Springer.

Mhajne, Anwar & Alexis Henshaw (eds.) (2024) *Critical Perspectives on Cybersecurity: Feminist and Postcolonial Interventions*. Oxford University Press.

Mhajne, Anwar & Crystal Whetstone (2024) "A feminist cybersecurity: addressing the crisis of cyber(in)security." *International Affairs* 100 (6): 2341-2360.

Mimran, Tal (2022) "Between Israel and Iran: Middle-East Attitudes to the Role of International Law in the Cyber-Sphere." *Baltic Yearbook of International Law Online* 20 (1): 209-235.

Monsees, Linda, Tobias Liebetrau, Jonathan Luke Austin, Anna Leander & Swati Srivastava (2023) "Transversal Politics of Big Tech." *International Political Sociology* 17 (1): olac020.

Moore, Daniel (2022) *Offensive Cyber Operations: Understanding Intangible Warfare*, London: Hurst & Company.

Möllers, Norma (2021) "Making Digital Territory: Cybersecurity, Techno-nationalism, and the Moral Boundaries of the State." *Science, Technology, & Human Values* 46 (1): 112-138.

Moret, Erica & Patryk Pawlak (2017) "The EU Cyber Diplomacy Toolbox: towards a cyber sanctions regime?" European Union Institute for Security Studies (EUISS) Brief, July 2017.

Mott, Gareth, Jason R.C. Nurse & Christopher Baker-Beall (2023) "Preparing for future cyber crises: lessons from governance of the coronavirus pandemic." *Policy Design and Practice*.

Moynihan, Harriet (2019) *The Application of International Law to State Cyberattacks: Sovereignty and Non-Intervention*, Chatham House.

Moynihan, Harriet (2020) "The vital role of international law in the framework for responsible state behaviour in cyberspace." *Journal of Cyber Policy*.

Mueller, Benjamin (2014) "The Laws of War and Cyberspace: On the Need for a Treaty Concerning Cyber Conflict." *Strategic Update 14.2*, London: London School of Economics and Political Science.

Mueller, Milton, Karl Grindal, Brenden Kuerbis & Farzaneh Badiei (2019) "Cyber Attribution: Can a New Institution Achieve Transnational Credibility?" *The Cyber Defense Review* 4 (1): 107-122.

Mukerji, Asoke (2020) "The Need for an International Convention on Cyberspace." *Horizons: Journal of International Relations and Sustainable Development* 16: 198-209.

Murray, Andrew (2007) *The Regulation of Cyberspace: Control in the Online Environment*, New York: Routledge.

Murray, Gregg R., and Craig Douglas Albert (2025) "In cyber we trust? Understanding election legitimacy in the age of electronic election systems." *Journal of Information Technology & Politics*.

Nakayama, Bryan (2022) "Democracies and the Future of Offensive (Cyber-Enabled) Information Operations." *The Cyber Defense Review* 7 (3): 49-65.

Nanni, Riccardo (2024) *Rising China and Internet Governance: Multistakeholderism, Fragmentation and the Liberal Order in the Age of Digital Sovereignty*. Springer.

Neilsen, Rhiannon (2023) "Coding protection: 'cyber humanitarian interventions' for preventing mass atrocities." *International Affairs* 99 (1): 299-319.

Nye, Joseph S. (2013) "From Bombs to Bytes: Can Our Nuclear History Inform Our Cyber Future?" *Bulletin of the Atomic Scientists* 69 (5): 8-14.

Nye, Joseph S. (2014) "The Regime Complex for Managing Global Cyber Activities. The Centre for International Governance." *Global Commission on Internet Governance, Paper Series: No. 1 – May*, Centre for International Governance Innovation (CIGI) and Chatham House.

Nye, Joseph S. (2018) *Normative Restraints on Cyber Conflict*, Cambridge, Mass.: Belfer Center for Science and International Affairs, Harvard Kennedy School.

Ohlin, Jens David (2020) *Election Interference: International Law and the Future of Democracy*, Cambridge University Press.

O'Loughlin, Ben & Alexi Drew (2020) "Sending a message: the primacy of action as communication in cyber-security." In: Dutton, W.H. (ed), *A Research Agenda for Digital Politics*, Elgar Research Agendas: 146-158.

Onderco, Michal (2025) "Navigating the AI frontier: Insights from the Ukraine conflict for NATO's governance role in military AI." *Journal of Strategic Studies*.

Oorsprong, Ferry, Paul Ducheine & Peter Pijpers (2023) "Cyber-attacks and the right of self-defense: a case study of the Netherlands." *Policy Design and Practice*.

Orji, Uchenna Jerome (2012) *Cybersecurity: Law and Regulation*, Wolf Legal Publishers.

Orji, Uchenna Jerome (2024) "Looking towards Europe? Assessing the prospects of the ECOWAS Cybersecurity Strategy in promoting responsible state behavior." *International Cybersecurity Law Review* 5: 143-168.

Ott, Nikolas (2017) "Conflict in Cyberspace: How International Legal Norms Can Reduce Military Escalation in Cyberspace." *Fletcher Security Review* 3 (1): 67-76.

Pawlak, Patryk (2016) "Confidence-Building Measures in Cyberspace: Current Debates and Trends." In: Osula, A.-M. & Rõigas, H. (eds), *International Cyber Norms: Legal, Policy & Industry Perspectives*, Tallinn: NATO CCD COE Publications, 129-153.

Pawlak, Patryk (2019) "The EU's Role in Shaping the Cyber Regime Complex." *European Foreign Affairs Review* 24 (2): 167–186.

Pawlak, Patryk (2023) "The pursuit of positive accountability in the cyber domain." *Global Policy*.

Pedersen, Frederik A.H. & Jeppe T. Jacobsen (2024) "Narrow windows of opportunity: the limited utility of cyber operations in war." *Journal of Cybersecurity* 10: tyae014.

Perarnaud, Clement & Julien Rossi (2023) "The EU and Internet standards – Beyond the spin, a strategic turn?" *Journal of European Public Policy*.

Permanent Monitoring Panel on Information Security of the World Federation of Scientists (WFS) (2010) "Erice Declaration on Principles for Cyber Stability and Cyber Peace." *International Seminar on Nuclear War and Planetary Emergencies: 42nd Session, Erice, Italy, 19-24 August*: 110-111.

Pijpers, Peter B.M.J. (2023) *Influence Operations in Cyberspace and the Applicability of International Law*. Elgar International Law and Technologies Series, Edward Elgar.

Pijpers, Peter B.M.J. (2023) "Careful What You Wish For: Tackling Legal Uncertainty in Cyberspace." *Nordic Journal of International Law* 92 (3): 394-421.

Polanski, Paul Przemyslaw (2006) "Towards a Supranational Internet Law." *Journal of International Commercial Law and Technology* 1 (1): 1-9.

Polanski, Paul Przemyslaw (2007) *Customary Law of the Internet. In the Search for a Supranational Cyberspace Law*, The Hague: TMC Asser Press.

Post, David G. (2000) "Of Black Holes and Decentralized Law-Making in Cyberspace." *Vanderbilt Journal of Entertainment Law & Practice* 2 (1): 70-79.

Qiao-Franco, Guangyu (2024) "An Emergent Community of Cyber Sovereignty: The Reproduction of Boundaries?" *Global Studies Quarterly* 4 (1).

Radu, Roxana (2023) "DNS4EU: a step change in the EU's strategic autonomy?" *Journal of Cyber Policy*.

Radu, Roxana & Cedric Amon (2021) "The governance of 5G infrastructure: between path dependency and risk-based approaches." *Journal of Cybersecurity* 7 (1).

Rauscher, Karl Frederick & Andrey Korotkov (2011) "Working Towards Rules for Governing Cyber Conflict. Rendering the Geneva and Hague Conventions in Cyberspace." EastWest Institute.

Raymond, Mark (2016) "Applying Old Rules to New Cases: International Law in the Cyber Domain." Paper presented to the International Studies Association, Atlanta GA, 16-19 March 2016.

Raymond, Mark & Justin Sherman (2023) "Authoritarian multilateralism in the global cyber regime complex: The double transformation of an international diplomatic practice." *Contemporary Security Policy*.

Reinhold, Thomas, Helene Pleil & Christian Reuter (2023) "Challenges for Cyber Arms Control: A Qualitative Expert Interview Study." *Zeitschrift für Außen- und Sicherheitspolitik* 16: 289-310.

Reinhold, Thomas & Christian Reuter (2023) "Preventing the escalation of cyber conflicts: towards an approach to plausibly assure the non-involvement in a cyber-attack." *Zeitschrift für Friedens- und Konfliktforschung*.

Ridout, T.A. (2016) "Here We Go Again: A Comparative Approach to Developing an International Cyberspace Governance Framework."

Riecke, Lena (2023) "Unmasking the Term 'Dual Use' in EU Spyware Export Control." *European Journal of International Law* 34 (3): 697-720.

Roguski, Przemysław (2020) *Application of International Law to Cyber Operations: A Comparative Analysis of States' Views*, The Hague Program for Cyber Norms Policy Brief, March 2020.

Romanosky, Sasha & Benjamin Boudreaux (2020) "Private-Sector Attribution of Cyber Incidents: Benefits and Risks to the U.S. Government." *International Journal of Intelligence and CounterIntelligence*: 1-31.

Ross, Cameron L. (2023) "Going nuclear: The development of American strategic conceptions about cyber conflict." *Journal of Strategic Studies.*

Rowe, N.C. (2018) "A Taxonomy of Norms in Cyberconflict for Government Policymakers." *Journal of Information Warfare* 17 (1): 31-48.

Ruck, Jan (2024) "A Geoeconomic Fix? European Industrial Policy on Semiconductors Amidst Global Competition." *Journal of Common Market Studies.*

Rusch, Jonathan J. (2000) "Cyberspace and the "Devil's Hatband"." *Seattle University Law Review* 24 (2): 577-598.

Rusinova, Vera & Ekaterina Martynova (2023) "Fighting Cyber Attacks with Sanctions: Digital Threats, Economic Responses." *Israel Law Review.*

Ryan, Julie J.C.H., Daniel J. Ryan & Eneken Tikk (2010) "Cybersecurity Regulation: Using Analogies to Develop Frameworks for Regulation." In; Tikk, E. & Talihärm, A-M. (eds), *International Cyber Security Legal & Policy Proceedings 2010*, Tallinn: NATO CCD COE, 76-99.

Sander, Barrie (2019) "Democracy Under The Influence: Paradigms of State Responsibility for Cyber Influence Operations on Elections." *Chinese Journal of International Law* 18 (1): 1–56.

Scharre, Paul (2023) *Four Battlegrounds: Power in the Age of Artificial Intelligence*, W.W. Norton.

Schjølberg, Stein & Solange Ghernaouti-Hélie (2009) *A Global Protocol on Cybersecurity and Cybercrime*, Cybercrimelaw.net.

Schjølberg, Stein & Solange Ghernaouti-Hélie (2011) *A Global Treaty on Cybersecurity and Cybercrime*, Cybercrimelaw.net.

Schmitt, Michael N. (2017) "Grey Zones in the International Law of Cyberspace." *The Yale Journal of International Law Online* 42 (2): 1-21.

Schmitt, Michael N. (2017) "Peacetime Cyber Responses and Wartime Cyber Operations Under International Law: An Analytical *Vade Mecum*." *Harvard National Security Journal* 8: 239-282.

Schmitt, Michael N. (2018) "\"Virtual\" Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law." *Chicago Journal of International Law* 19 (1): 30-67.

Schmitt, Michael N. (2019) "Wired Warfare 3.0: Protecting the Civilian Population During Cyber Operations." *International Review of the Red Cross*: 1-23.

Schmitt, Michael N. (2020) "Autonomous Cyber Capabilities and the International Law of Sovereignty and Intervention." *International Law Studies* 96: 549-576.

Schmitt, Michael N. & Liis Vihul (2014) "The Nature of International Law Cyber Norms." *Tallinn Paper No. 5, Special Expanded Issue*, Tallinn: NATO CCD COE Publications.

Schmitt, Michael N. & Liis Vihul (2017) "Respect for Sovereignty in Cyberspace." *Texas Law Review* 95: 1639-1670.

Schmitt, Michael N. & Liis Vihul (2017) "Sovereignty in Cyberspace: *Lex Lata Vel Non?*." *AJIL Unbound* 111: 213-218.

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

Schmitt, Michael N. (ed) (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge: Cambridge University Press.

Schmitt, Michael N. | Ministerie van Defensie (2018) *International Cyber Norms: Reflections on the Path Ahead*, Ministerie van Defensie.

Schneider, Jacquelyn & Julia Macdonald (2023) "Looking back to look forward: Autonomous systems, military revolutions, and the importance of cost." *Journal of Strategic Studies*.

Shackelford, Scott J. (2020) *Governing New Frontiers in the Information Age: Toward Cyber Peace,* Cambridge University Press.

Shackelford, Scott J. (2021) "Inside the Drive for Cyber Peace: Unpacking Implications for Practitioners and Policymakers." *UC Davis Business Law Journal* 21 (285).

Shapiro, Scott J. (2023) *Fancy Bear Goes Phishing: The Dark History of the Information Age, in Five Extraordinary Hacks*. Macmillan.

Sharma, Chinmayi (2022) "Tragedy of the Digital Commons." *North Carolina Law Review* (forthcoming/available at SSRN).

Sherman, Justin (2023) *Cybersecurity under the Ocean: Submarine Cables and US National Security*, Hoover Institution, Aegis Series Paper No. 2301.

Shires, James (2021) *The Politics of Cybersecurity in the Middle East*, Hurst.

Shires, James (2021) "Windmills of the Mind: Higher-Order Forms of Disinformation in International Politics." In: Jancárková, T., Lindström, L., Visky, G. & Zotz, P. (eds), *2021 13th International Conference on Cyber Conflict: Going Viral*, Tallinn: NATO CCD COE Publications.

Shires, James (2023) "Career connections: transnational expert networks and multilateral cybercrime negotiations." *Contemporary Security Policy*.

Singh, Harsha Vardhana, Ahmed Abdel-Latif & L. Lee Tuthill (2016) "Governance of International Trade and the Internet: Existing and Evolving Regulatory Systems." *Global Commission on Internet Governance, Paper Series: No. 32 – May*, Centre for International Governance Innovation (CIGI) and Chatham House.

Slayton, Rebecca, and Lilly Muller (2025) "Coordinating uncertainty in the political economy of cyber threat intelligence." *Social Studies of Science*.

Slupska, Julia (2020) "War, Health & Ecosystem: Generative Metaphors in Cybersecurity Governance." *Philosophy & Technology*, forthcoming. (Pre-print available at SSRN: https://ssrn.com/abstract=3534579).

Smeets, Max (2019) "There Are Too Many Red Lines in Cyberspace." *Lawfare* (20 March 2019).

Smeets, Max (2020) "US cyber strategy of persistent engagement & defend forward: implications for the alliance and intelligence collection." *Intelligence and National Security* 35 (3): 444-453.

Smeets, Max (2022) "Cyber Arms Transfer: Meaning, Limits, and Implications." *Security Studies* 31 (1): 65-91.

Smeets, Max (2022) *No Shortcuts: Why States Struggle to Develop a Military Cyber-Force*, London: Hurst & Company.

Smeets, Max (2025) *Ransom War: How Cyber Crime Became a Threat to National Security*. Hurst Publishers.

Smith, Hanna (2023) "The geopolitics of cyberspace and the European Union's changing identity." *Journal of European Integration* 45 (8): 1219-1234.

Sofaer, Abraham D., David Clark & Whitfield Diffie (2010) "Cyber Security and International Agreements." *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*, National Academies Press, 179-206.

Solar, Carlos (2020) "Cybersecurity and cyber defence in the emerging democracies." *Journal of Cyber Policy* 5 (3): 392-412.

Solum, Lawrence B. & Minn Chung (2004) "The Layers Principle: Internet Architecture and the Law." *Notre Dame Law Review* 79 (3): 815-948.

Steinbruner, John (2011) "Prospects for Global Restraints on Cyberattack." *Arms Control Today* 41 (10): 21-26.

Stevens, Tim (2012) "A Cyberwar of Ideas? Deterrence and Norms in Cyberspace." *Contemporary Security Policy* 33 (1): 148-170.

Stevens, Tim (2020) "United Kingdom: Pragmatism and adaptability in the cyber realm." In: Romaniuk, S.N. & Manjikian, M., *The Routledge Companion to Global Cyber-Security Strategy*, Basingstoke: Palgrave MacMillan.

Streltsov, A.A. (2007) "International Information Security: Description and Legal Aspects." In: Vignard, K. (ed), *Disarmament Forum: ICTs and International Security*, Geneva: UNIDIR, 2007 (3): 5-14.

Sukumar, Arun, and Arindrajit Basu (2024) "Back to the territorial state: China and Russia's use of UN cybercrime negotiations to challenge the liberal cyber order." *Journal of Cyber Policy* 9 (2): 256-287.

Taddeo, Mariarosaria (2017) "Deterrence by Norms to Stop Interstate Cyber Attacks." *Minds and Machines* 27 (3): 387-392.

Taddeo, Mariarosaria (2018) "Deterrence and Norms to Foster Stability in Cyberspace." *Philosophy & Technology* 31: 323-329.

Taddeo, Mariarosaria (2020) "Norms and Strategies for Stability in Cyberspace." In: Burr, C. & Milano, S. (eds), *The 2019 Yearbook of the Digital Ethics Lab*, Digital Ethics Lab Yearbook: Springer.

Taillat, Stéphane (2019) "Disrupt and restraint: The evolution of cyber conflict and the implications for collective security." *Contemporary Security Policy* 40 (3): 368-381.

Tennant, Ian & Ana Paula Oliveira (2024) "Applying the right lessons from the negotiation and implementation of the UNTOC and the UNCAC to the implementation of the newly agreed UN 'cybercrime' treaty." *Journal of Cyber Policy*.

Thornton, Rod & Marina Miron (2022) "Winning Future Wars: Russian Offensive Cyber and Its Vital Importance in Moscow's Strategic Thinking." *The Cyber Defense Review* 7 (3): 117-135.

Tikk, Eneken (2011) "Ten Rules for Cyber Security." *Survival* 53 (3): 119-132.

Tikk-Ringas, Eneken (2012) "Developments in the Field of Information and Telecommunication in the Context of International Security: Work of the UN First Committee 1998-2012." *Cyber Policy Process Brief*, ICT4Peace Foundation.

Tikk-Ringas, Eneken (2015) "Legal Framework of Cyber Security." In: Lehto, M. & Neittaanmäki, P. (eds), *Cyber Security: Analytics, Technology and Automation*, Springer International Publishing.

Tikk-Ringas, Eneken (2017) "International Cyber Norms Dialogue as an Exercise of Normative Power." *Georgetown Journal of International Affairs* 17 (3): 47-59.

Tikk-Ringas, Eneken (ed) (2015) *Evolution of the Cyber Domain: The Implications for National and Global Security - Strategic Dossier*, IISS-Routledge, "Chapter 5: The 2000s."

Tropina, Tatiana (2024) "'This is not a human rights convention!': the perils of overlooking human rights in the UN cybercrime treaty." *Journal of Cyber Policy*.

Tropina, Tatiana & Cormac Callanan (2015) *Self- and Co-regulation in Cybercrime, Cybersecurity and National Security*, Springer.

Tsagourias, Nicholas (2016) "Non-State Actors, Ungoverned Spaces and International Responsibility for Cyber Acts." *Journal of Conflict and Security Law* 21 (3): 455-474.

Tsagourias, Nicholas, Russell Buchan, and Daniel Franchini (eds.) (2024) *The Peaceful Settlement of Inter-State Cyber Disputes*. Hart Publishing.

Valeriano, Brandon (2022) "The Failure of the Offense/Defense Balance in Cyber Security." *The Cyber Defense Review* 7 (3): 91-101.

Vallor, Shannon (2024) *The AI Mirror: How to Reclaim Our Humanity in an Age of Machine Thinking*. Oxford University Press.

Vecellio Segate, Riccardo (2019) "Fragmenting Cybersecurity Norms Through the Language(s) of Subalternity: India in 'the East' and the Global Community." *Columbia Journal of Asian Law* 32 (2): 78-138. (Available at SSRN: https://ssrn.com/abstract=3392781).

Vićić, Jelena & Richard Harknett (2024) "Identification-imitation-amplification: understanding divisive influence campaigns through cyberspace." *Intelligence and National Security*.

Vishik, Claire, Mihoko Matsubara & Audrey Plonk (2016) "Key Concepts in Cyber Security: Towards a Common Policy and Technology Context for Cyber Security Norms." In: Osula, A.-M. & Rõigas, H. (eds), *International Cyber Norms: Legal, Policy & Industry Perspectives*, Tallinn: NATO CCD COE Publications, 221-242.

Wagnsson, Charlotte, Maria Hellman and Aiden Hoyle (2024) "Securitising information in European borders: how can democracies balance openness with curtailing Russian malign information influence." *European Security*.

Walker, Clive & Ummi Hani Binti Masood (2020) "Domestic Law Responses to Transnational Cyberattacks and Other Online Harms: Internet Dreams Turned to Internet Nightmares and Back Again." *Notre Dame Journal of International & Comparative Law* 10 (1).

Walker, Paul A. (2015) "Law of the Horse to Law of the Submarine: The Future State Behavior in Cyberspace." In: Maybaum, M., Osula, A.-M., & Lindström, L. (eds), *2015 7th International Conference on Cyber Conflict: Architectures in Cyberspace*, Tallinn: NATO CCD COE Publications, 93-104.

Watts, Sean (2016) "Cyber Law Development and the United States Law of War Manual." In: Osula, A.-M. & Rõigas, H. (eds), *International Cyber Norms: Legal, Policy & Industry Perspectives*, Tallinn: NATO CCD COE Publications, 49-63.

Weiss, Moritz (2022) "The rise of cybersecurity warriors?" *Small Wars & Insurgencies* 33 (1-2): 272-293.

Weiss, Moritz, and Nicolas Krieger (2025) "The political economy of cybersecurity: Governments, firms and opportunity structures for business power." *Contemporary Security Policy*.

Whetstone, Crystal, and K.C. Luna (2024) "A Call for Feminist Insights in Cybersecurity: Implementing United Nations Security Council Resolution 1325 on Women, Peace, and Security in Cyberspace". In: *Critical Perspectives on Cybersecurity: Feminist and Postcolonial Interventions*, edited by Anwar Mhajne and Alexis Henshaw.

Whyte, Christopher (2018) "Dissecting the Digital World: A Review of the Construction and Constitution of Cyber Conflict Research." *International Studies Review* 20 (3): 520-532.

Willett, Marcus (2019) "Assessing Cyber Power." *Survival* 61 (1): 85-90.

Willett, Marcus (2024) *Cyber Operations and Their Responsible Use*. London: Routledge.

Wilner, Alex S. (2020) "US cyber deterrence: Practising guiding theory." *Journal of Strategic Studies* 43 (2): 245-280.

Wingfield, Thomas C. & Eneken Tikk (2010) "Frameworks for International Cyber Security: The Cube, the Pyramid, and the Screen." In: Tikk, E. & Talihärm, A-M. (eds), *International Cyber Security Legal & Policy Proceedings 2010*, Tallinn: NATO CCD COE, 16-23.

Wolff, Josephine (2022) *Cyberinsurance Policy: Rethinking Risk in an Age of Ransomware, Computer Fraud, Data Breaches, and Cyberattacks*, MIT Press.

Wolff, Josephine (2023) "The role of insurers in shaping international cyber-security norms about cyber-war." *Contemporary Security Policy*.

Woods, Daniel W. & Jessica Weinkle (2020) "Insurance definitions of cyber war." *The Geneva Papers on Risk and Insurance - Issues and Practice* 45: 639-656.

Work, J.D. (2022) "Burned and Blinded: Escalation Risks of Intelligence Loss from Countercyber Operations in Crisis." *International Journal of Intelligence and CounterIntelligence*.

Yilmaz, Murat (2024) "Gendered Transnational Authoritarianism in Cyberspace: A Case Study of the Uyghurs". In: *Critical Perspectives on Cybersecurity: Feminist and Postcolonial Interventions*, edited by Anwar Mhajne and Alexis Henshaw.

Zafar, Ammar (2025) "Reconciling blockchain technology and data protection laws: regulatory challenges, technical solutions, and practical pathways." *Journal of Cybersecurity* 11 (1): tyaf002.

Zegart, Amy B. (2022) *Spies, Lies, and Algorithms: The History and Future of American Intelligence*, Princeton University Press.

This bibliography was originally started and compiled by Liisi Adamson and is maintained by the team from The Hague Program on International Cyber Security (formerly The Hague Program for Cyber Norms) - please send any additions or suggestions to info@thehagueprogram.nl

Zhu, Lixin, & Wei Chen (2022) "Chinese Approach to International Law with Regard to Cyberspace Governance and Cyber Operation: From the Perspective of the Five Principles of Peaceful Co-existence." *Baltic Yearbook of International Law Online* 20 (1): 187-208.

Zilincik, Samuel & Isabelle Duyvesteyn (2023) "Strategic studies and cyber warfare." *Journal of Strategic Studies*.

Ziolkowski, Katharina (2013) *Confidence Building Measures for Cyberspace – Legal Implications*, Tallinn: NATO CCD COE Publications.

Ziolkowski, Katharina (ed) (2013) *Peacetime Regime for State Activities in Cyberspace, International Law, International Relations and Diplomacy*, Tallinn: NATO CCD COE Publications.

Zittrain, Jonathan L. (2008) *The Future of the Internet and How to Stop It*, New Haven: Yale University Press.

Zúñiga, Nicholas, Saheli Datta Burton, Filippo Blancato, and Madeline Carr (2024) "The Geopolitics of Technology Standards: Historical Context for US, EU and Chinese Approaches." *International Affairs* 100 (4).

This bibliography was originally started and compiled by Liisi Adamson and is maintained by the team from The Hague Program on International Cyber Security *(formerly The Hague Program for Cyber Norms) - please send any additions or suggestions to* *info@thehagueprogram.nl*