

## Cyber Bibliography, 2024 mjf

- Allegri, Riccardo. "Russian Full Spectrum Conflicts and Information Warfare as Complex Adaptive Systems: The 2014 Crimean Case Study." *Comparative Strategy* 42:4 (2023): 528-555.
- Arquilla, John. *Bitskrieg: The New Challenge of Cyberwarfare*. Medford: Polity, 2021.
- and David Ronfeldt. "Cyberwar is Coming!" *Comparative Strategy* 12, no. 2 (Spring 1993): 141-165. <https://doi.org/10.1080/01495939308402915>
- Barrinha, André and Thomas Renard. "Power and Diplomacy in the Post-liberal Cyberspace." *International Affairs* 96:3 (2020): 749-766. <https://doi.org/10.1093/ia/iiz274>
- and Rebecca Turner. "Strategic Narratives and the Multilateral Governance of Cyberspace: The Cases of European Union, Russia, and India." *Contemporary Security Policy* 45:1 (2024): 72-109.
- Betz, David. *Carnage and Connectivity: Landmarks in the Decline of Conventional Military Power*. New York, NY: Oxford University Press, 2015.
- Blumler, Jay and Stephen Coleman. *The Internet and Democratic Citizenship: Theory, Practice and Policy*. New York: Cambridge University, 2009.
- Borghard, Erica D. and Shawn N. Lonergan. "The Logic of Coercion in Cyberspace." *Security Studies* Vol. 26, No. 3 (2017): 452-481. <https://doi.org/10.1080/09636412.2017.1306396>
- Brantly, Aaron Franklin. "The Cyber Losers." *Democracy and Security* 10, no. 2 (2014): 132-155. <https://www.jstor.org/stable/48602334>
- Brenner, Joel. *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare*. New York, NY: Penguin Press, 2011.
- Brenner, Susan W. *Cyberthreats: The Emerging Fault Lines of the Nation States*. New York: NY: Oxford University Press, 2009.
- Buchanan, Ben. *The Cybersecurity Dilemma: Hacking, Trust, and Fear Between Nations*. New York, NY: Oxford University Press, 2016.
- Burton, Joe and George Christou. "Bridging the Gap Between Cyberwar and Cyberpeace." *International Affairs* 97:6 (2021): 1727-1747. <https://doi.org/10.1093/ia/iiab172>
- Chernobrov, Dmitry. "Diasporas as Cyberwarriors: Infopolitics, Participatory Warfare and the 2020 Karabakh War." *International Affairs* 98:2 (2022): 631-651. <https://doi.org/10.1093/ia/iia015>
- Choucri, Nazli. *Cyberpolitics in International Relations*. Cambridge, MA: MIT Press, 2012.
- Clarke, Richard and Robert K. Knake. *Cyber War: The Next Threat to National Security and What to do About It*. New York, NY: HarperCollins, 2010.
- Crosston, Matthew D. "World Gone Cyber MAD: How 'Mutually Assured Debilitation' Is the Best Hope for Cyber Deterrence." *Strategic Studies Quarterly* (Spring 2011): 100-116.
- Deibert, Ronald J. *Black Code: Inside the Battle for Cyberspace*. Toronto: McClelland & Stewart, 2013.
- "The Road to Digital Unfreedom: Three Painful Truths About Social Media." *Journal of Democracy* 30, no. 1 (Jan 2019): 40-52. <https://www.journalofdemocracy.org/articles/the-road-to-digital-unfreedom-three-painful-truths-about-social-media/>

- Demchak, Chris C. "Defending Democracies in a Cybered World." *Brown Journal of World Affairs* Vol. 24, Issue 1 (Fall/Winter 2017): 139-158.  
<https://www.jstor.org/stable/27119084>
- . *Wars of Disruption and Resilience: Cybered Conflict, Power, and National Security*. Athens, GA: University of Georgia, 2012.
- and Peter Dembrowski. "Rise of a Cybered Westphalian Age." *Strategic Studies Quarterly* (Spring 2011): 32-61. DOI:[10.1007/978-3-642-55007-2\\_5](https://doi.org/10.1007/978-3-642-55007-2_5)
- DeNardis, Laura. *The Global War for Internet Governance*. New Haven, CT: Yale University Press, 2014.
- Diamond, Larry. "Liberation Technology." *Journal of Democracy* 21, no. 3 (July 2010): 69-83.  
<https://www.journalofdemocracy.org/articles/liberation-technology/>
- Ferguson, Niall. *The Square and the Tower: Networks and Power, from the Freemasons to Facebook*. New York: Penguin Press, 2018.
- Finlay, Christopher J. "Just War, Cyber War, and the Concept of Violence." *Philosophy and Technology* 31:4 (2018): 357-377.
- Fischerkeller, Michael P. and Richard J. Harknett. "Deterrence is Not a Credible Strategy for Cyberspace." *ORBIS* 61, 3 (Summer 2017): 381-393.  
<https://doi.org/10.1016/j.orbis.2017.05.003>
- Flonk, Daniëlle. "Emerging Illiberal Norms: Russia and China as Promoters of Internet Content Control." *International Affairs* 97:6 (2021): 1925-1944. <https://doi.org/10.1093/ia/iiab146>
- Flynn, Matthew J. "Civilians 'Defending Forward' in Cyberspace: Aligning Cyber Strategy and Cyber Operations." *The Cyber Defense Review* (Winter 2020): 29-39.  
<https://cyberdefensereview.army.mil/CDR-Content/Articles/Article-View/Article/2121707/civilians-defending-forward-in-cyberspace-aligning-cyber-strategy-and-cyber-ope/>.
- . "The Cyber 'Errand into the Wilderness': The 'Defending Forward' Inflection Point." *Georgetown Journal of International Affairs* Vol. 21 (Fall 2020): 71-79.  
[10.1353/gia.2020.0015](https://doi.org/10.1353/gia.2020.0015).
- . "Cyber Rebellions: The Online Struggle for Openness." *Journal of International Affairs*, 71, no. 1.5 (Special Issue 2018): 107-114.  
<https://jia.sipa.columbia.edu/cyber-rebellions-online-struggle-openness>
- . "Strategic Cyber: Responding to Russian Online Information Warfare." *The Cyber Defense Review*, Special Edition (2019): 193-207.  
<https://www.jstor.org/stable/26846128>.
- . "Winning the Digital War: Cyber Ideology and the Spectrum of Conflict." *Journal of Strategic Security* 14, 4 (2021): 87-102. <https://doi.org/10.5038/1944-0472.14.4.1968>.
- Gartzke, Erik and Jon R. Lindsay. "Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace." *Security Studies*, 24: 2 (2015): 316-348.  
<http://dx.doi.org/10.1080/09636412.2015.1038188>
- Haner, Justin K. and Robert K. Knake. "Breaking Botnets: A Quantitative Analysis of Individual, Technical, Isolationist, and Multilateral Approaches to Cybersecurity." *Journal of Cybersecurity* 00,0 (2021): 1-15.

- Harknett, Richard J. and Max Smeets. "Cyber Campaigns and Strategic Outcomes." *Journal of Strategic Studies* 45:4 (2022): 534-567. <https://doi.org/10.1080/01402390.2020.1732354>
- . "Is Deterrence Possible in Cyberspace?" Correspondence, Richard J. Harknett and Joseph Nye. *International Security* 42 no. 2 (Fall 2017): 196-199. [https://doi.org/10.1162/ISEC\\_c\\_00290](https://doi.org/10.1162/ISEC_c_00290)
- Harris, Shane. *@War: The Rise of the Military-Internet Complex*. New York, NY: Houghton Mifflin Harcourt, 2014.
- Healey, Jason, ed. *A Fierce Domain: Conflict in Cyberspace, 1986-2012*. Arlington, VA: Cyber Studies Association, 2013.
- . "Claiming the Lost Cyber Heritage." *Strategic Studies Quarterly* (Fall 2012): 11-19.
- . "The Implications of Persistent (and Permanent) Engagement in Cyberspace." *Journal of Cybersecurity* 5, no. 1 (2019): 1-15. <https://doi.org/10.1093/cybsec/tyz008>
- Heineeg, Wolff Heintschel von. "Territorial Sovereignty and Neutrality in Cyberspace." *International Law Studies* 89 (US Naval War College, Study 123, 2013): 123-156. <https://digital-commons.usnwc.edu/ils/vol89/iss1/17/>
- Junio, Timothy J. "How Probable is Cyber War?: Bringing IR Theory Back in to the Cyber Conflict Debate." *Journal of Strategic Studies* 36, no. 1 (2013): 125-133. <http://dx.doi.org/10.1080/01402390.2012.739561>
- Kaplan, Fred. *Dark Territory: The Secret History of Cyber War*. New York, NY: Simon & Shuster, 2016.
- Klimburg, Alexander. *The Darkening Web: The War for Cyberspace*. New York, NY: Penguin, 2017.
- Kostyuk, Nadiya and Aaron Brantly. "War in the Borderland Through Cyberspace: Limits of Defending Ukraine Through Interstate Cooperation." *Contemporary Security Policy* 43:3 (2022): 498-515. <https://doi.org/10.1080/13523260.2022.2093587>.
- Leuprecht, Christian, Joseph Szeman, and David B. Skillicoen. "The Damoclean Sword of Offensive Cyber: Policy Uncertainty and Collective Insecurity." *Contemporary Security Policy* 40:3 (2019): 382-407. <https://doi.org/10.1080/13523260.2019.1590960>
- Libicki, Martin C. *Conquest in Cyberspace: National Security and Information Warfare*. New York: Cambridge University, 2007.
- . *Cyberdeterrence and Cyberwar*. Santa Monica, CA: RAND Corp., 2009. [https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND\\_MG877.pdf](https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf);
- . *Cyberspace in Peace and War*. 2<sup>nd</sup> ed. Annapolis, MD: Naval Institute Press, 2021.
- Lin, Herbert, Amy Zegart, eds. *Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations*. Washington, DC: Brookings Institution Press, 2018.
- Lindsay, Jon R. and Erik Gartzke. *Elements of Deterrence: Strategy, Technology, and Complexity in Global Politics*. New York, NY: Oxford University Press.
- Lynn, William J. "Defending a New Domain." *Foreign Affairs*, 89, 5 (2010): 97-108.
- MacKinnon, Rebecca. *Consent of the Networked: The Worldwide Struggle for Internet Freedom*. New York, NY: Basic Books, 2012.

- Mazanec, Brian M. *The Evolution of Cyber War: International Norms for Emerging-Technology Weapons*. Lincoln: Potomac Books, 2015.
- . *Understanding Cyber Warfare: Politics, Policy, and Strategy*. 2<sup>nd</sup> ed. New York, NY: Routledge, 2023.
- Morozov, Evgeny. *The Net Delusion: The Dark Side of Internet Freedom*. New York, NY: Public Affairs, 2011.
- Mosco, Vincent. *Becoming Digital: Towards a Post-Internet Society*. Bingley: Emerald Publishing, 2017.
- Mueller, Milton L. *Networks and States: The Global Politics of Internet Governance*. Cambridge, Mass: MIT Press, 2010.
- Nakasone, Paul M. "A Cyber Force for Persistent Operations." *Joint Force Quarterly* 92 (1<sup>st</sup> Quarter 2019): 10-14.  
[https://cs.brown.edu/courses/cs180/sources/2019\\_01\\_22\\_JFQ\\_CyberRoleForPersistentOperations\\_Nakasone.pdf](https://cs.brown.edu/courses/cs180/sources/2019_01_22_JFQ_CyberRoleForPersistentOperations_Nakasone.pdf)
- Nye, Joseph. "Deterrence and Dissuasion in Cyberspace." *International Security* 41, no. 3 (Winter 2016-2017): 44-71. doi:10.1162/ISEC\_a\_00266
- . "Nuclear Lessons for Cyber Security?" *Strategic Studies Quarterly* (Winter 2011): 18-38.
- Rattray, Greg. *Strategic Warfare in Cyberspace*. Cambridge: MIT Press, 2008.
- Reveron, Derek S. ed. *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*. Washington, DC: Georgetown University Press, 2012.
- . *Security in the Cyber Age: An Introduction to Policy and Technology*. New York, NY: Cambridge University Press, 2024.
- Rheingold, Howard. *The Virtual Community: Homesteading on the Electronic Frontier*. Rev. ed. Cambridge, Mass: MIT Press, 1993, 2000.
- Rid, Thomas. *Cyber War Will Not Take Place*. New York: Oxford University, 2013.
- Rosenberger, Laura and Lindsay Gorman. "How Democracies Can Win the Information Contest." *The Washington Quarterly* (Summer 2020): 75-96.  
<https://doi.org/10.1080/01636660X.2020.1771045>
- Rosenzweig, Paul. *Cyber Warfare: How Conflicts in Cyberspace are Challenging America and Changing the World*. Santa Barbara, CA: Praeger, 2013.
- Sanger, David E. *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age*. New York, NY: Crown, 2018.
- Shackelford, Scott J., Frederick Douzet, and Christopher Ankerson, eds. *Cyber Peace: Charting a Path Toward a Sustainable, Stable, and Secure Cyberspace*. New York, NY: Cambridge University Press, 2022.
- Shandler, Ryan, Michael L. Gross and Daphna Canetti. "A Fragile Public Preference for Cyber Strikes: Evidence from Survey Experiments in the United States, United Kingdom, and Israel." *Contemporary Security Policy* 42:2 (2021): 135-162.  
<https://doi.org/10.1080/13523260.2020.1868836>
- Sharma, Amit. "Cyber Wars: A Paradigm Shift from Means to Ends." In *The Virtual Battlefield: Perspectives on Cyber Warfare*, ed. Christian Czosseck and Kenneth Geers. Amsterdam: IOS Press, 2009.

- Sharp, Travis. "Theorizing Cyber Coercion: The 2014 North Korean Operation Against Sony." *Journal of Strategic Studies* 40, no. 7 (2017): 1-29. <https://doi.org/10.1080/01402390.2017.1307741>
- Singer, P.W. and Allan Friedman. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. New York, NY: Oxford University Press, 2014.
- Slayton, Rebecca. "What is the Cyber-Offense-Defense Balance?: Conceptions, Causes, and Assessments." *International Security* 41:3 (Winter 2017-2017): 72-109. <https://www.jstor.org/stable/26777791>
- Smeets, Max. "The Strategic Promise of Offensive Cyber Operations." *Strategic Studies Quarterly* 12, no. 3 (Fall 2018): 80-113. <https://www.jstor.org/stable/26481911>
- Solar, Carlos. "Cybersecurity and Cyber Defence in the Emerging Democracies." *Journal of Cyber Policy*, 5:3 (2020): 392-412. <https://doi.org/10.1080/23738871.2020.1820546>
- Stavridis, James G. and Elton C. Parker. "Sailing the Cyber Ship." *Joint Force Quarterly* Issue 65 (2<sup>nd</sup> Quarter 2012): 61-67.
- Sterner, Eric. "Retaliatory Deterrence in Cyberspace." *Strategic Studies Quarterly* (Spring 2011): 62-80.
- Stone, John. "Cyber War Will Take Place!" *Journal of Strategic Studies*, 36, no. 1 (2013): 101-108. <http://dx.doi.org/10.1080/01402390.2012.730485>
- Sukumar, Arun, Dennis Broeders, and Monica Kello. "The Pervasive Informality of the International Cybersecurity Regime: Geopolitics, Non-state Actors and Diplomacy." *Contemporary Security Policy* 45:1 (2024): 7-44.
- Valeriano, Brandon, Benjamin Jensen, and Ryan C. Maness. *Cyber Strategy: The Evolving Character of Power and Coercion*. New York, NY: Oxford University Press, 2018.
- and Ryan C. Maness. *Cyber War Versus Cyber Realities: Cyber Conflict in the International System*. New York, NY: Oxford University Press, 2015.
- Whyte, Christopher. "Cyber Conflict or Democracy 'Hacked'? How Cyber Operations Enhance Information Warfare." *Journal of Cybersecurity* (2020): 1-17. <https://doi.org/10.1093/cybsec/tyaa013>
- , "Cyberspace is What States Make of It: The Social Construction (and Deconstruction) of Strategic Concepts." *Comparative Strategy* 42, no. 1 (2023): 128-151. <https://doi.org/10.1080/01495933.2022.2158031>
- , A. Trevor Thrall, and Brian M. Mazanec, eds. *Information Warfare in the Age of Cyber Conflict*. New York, NY: Routledge, 2021.
- Wolfe, Josephine. "The Role of Insurers in Shaping International Cyber-security Norms about Cyber-war." *Contemporary Security Policy* 45:1 (2024): 141-170.
- Zilincik, Samuel and Isabelle Duyvesteyn. "Strategic Studies and Cyber Warfare." *Journal of Strategic Studies* 46:4 (2023): 836-857.