**Cyber Warfare:**
**Bibliography**
**Dr. Matthew J. Flynn 3/22**

TOPICS

Defining Cyber Warfare
  Cyber War, Histories
US Policy in Cyberspace
Cyber Operations
  Russia and Estonia
  Russian-Georgian Cyber War
  Stuxnet
Cyber Ideology (the Information/Cognitive War)
  China, the Great Firewall
  The Arab Spring and Social Media
  Other: North Korea & Venezuela
  ISIS, Online Terrorism
  Russia and Gray Zone Conflict
China and Cyber Warfare
Cyber Deterrence
Cyber as a Domain
Norming Cyberspace

**Defining Cyber Warfare**


"Cyber Roundtable: Cyber War." *Journal of Strategic Studies*, Vol. 36, Issue 1 (2013): 101-142.

Buchanan, Ben. *The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations*. New York: Oxford University, 2017. Pp. 304.

Carr, Jeffrey. *Inside Cyber Warfare*. O'Reilly, 2010. Pp. 212.

Clarke, Richard A. and Robert K. Knake. *Cyber War: The Next Threat to National Security and What to Do About It.* New York: HarperCollins Publishers, 2010. Pp. 290.

Flynn, Matthew J. "Information as the Cyber War. Literature Review." *MCU Journal*, Vol. 9, No. 2 (2018): 204-208.

----------. "Is There a Cyber? A Review Essay." *National Cyber Security Institute Journal*, Vol. 1, No. 2 (2014): 5-8.

----------. "Winning the Digital War: Cyber Ideology and the Spectrum of Conflict." *Journal of Strategic Security* Vol. 14, No. 4 (2021): 87-102.

Gartzke, Erik. "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth." *International Security*, Vol. 38, No. 2 (Fall 2013): 41-73.

---------- and Jon Lindsay. "Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace." *Security Studies*, Vol. 24, No. 2 (2015): 316-348.

Kello, Lucas. "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft." *International Security*, Vol. 38, No. 2 (Fall 2013): 7-40.

Libicki, Martin C. *Cyberspace in Peace and War*. Annapolis, MD: Naval Institute Press, 2016. Pp. 616.

----------. "The Specter of Non-Obvious Warfare." *Strategic Studies Quarterly* (Fall 2012): 88-101.

Liff, Adam P. "Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War." *The Journal of Strategic Studies*, Vol. 35, No. 3 (June 2012): 401-428.

Lindsay, Jon R. and Lucas Kello. "Correspondence: A Cyber Disagreement." *International Security*, Vol. 39, No. 2 (Fall 2014): 181-192.

Lonsdale, David J. *The Nature of War in the Information Age: Clausewitzian Future Strategy and History*. Eds. Colin Gray and Williamson Murray. London: Frank Cass, 2004. Pp. 263.

Reveron, Derek S., ed. *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World.* Georgetown University Press, 2012. Pp. 246.

Rid, Thomas. *Cyber War Will Not Take Place*. Oxford University Press, 2013. Pp. 207.

----------. "Cyber War Will Not Take Place." *Journal of Strategic Studies*, Vol. 35, No. 1 (2012): 5-32.

----------. "Think Again: Cyber War." *Foreign Policy Magazine* (March/April 2012): online. http://foreignpolicy.com/2012/02/27/think-again-cyberwar/

Rustici, Ross M. "Cyberweapons: Leveling the International Playing Field." *Parameters* (Autumn 2011): 32-42.

Singer, Peter and Alan Friedman. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. New York: Oxford University, 2014. Pp. 306.

Stephenson, Scott. "The Revolution in Military Affairs: 12 Observations on an Out-of-Date Idea." *Military Review* (May-June 2010): 38-46.

***Cyber War, Histories***

Bowden, Mark. *Worm: The First Digital World War*. New York: Atlantic Monthly Press, 2011. Pp. 241. (Conficker virus)

Harris, Shane. *@WAR: The Rise of the Military-Internet Complex*. New York: Houghton Mifflin Harcourt, 2014. Pp. 263.

Healey, Jason, ed. *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*. Arlington, VA: Cyber Conflict Studies Association, 2013. Pp. 352.

Kaplan, Fred. *Dark Territory: The Secret History of Cyber War*. New York: Simon & Schuster, 2016. Pp. 338.

Klimburg, Alexander. *The Darkening Web: The War for Cyberspace*. New York: Penguin, 2017. Pp. 420.

Sanger, David E. *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age*. New York: Crown, 2018. Pp. 357.

Stoll, Clifford. *The Cuckoo's Egg: Tracking a Spy Through a Maze of Computer Espionage*. New York: Doubleday, 1989. Pp. 326.

Warner, Michael. ''Cybersecurity: A Pre-History.'' *Intelligence and National Security*, 27, No. 5 (2012): 781–799.

**US Policy in Cyberspace**

Alexander, Keith B., Janet Jaffer, and Jennifer S. Brunet. "Clear Thinking About Protecting the Nation in the Cyber Domain." *The Cyber Defense Review*, Vol. 2, No.1 (Spring 2017): 29-38.

----------, Emily Goldman, Michael Warner. "Defending America in Cyberspace." *The National Interest*, No 128 (Nov/Dec 2013): 18-24.

Betz, David. "Cyberpower in Strategic Affairs: Neither Unthinkable Nor Blessed." *The Journal of Strategic Studies*, Vol. 35, No. 5 (Oct 2012): 689-711.

Carr, Madeline. "Public-Private Partnerships in National Cyber-security Strategies." *International Affairs*, Vol. 92, No. 1 (2016): 43-62.

Chertoff, Michael. "The Strategic Significance of the Internet Commons." *Strategic Studies Quarterly* (Summer 2014): 10-16.

Demchak, Chris C. and Peter Dombrowski. "Rise of a Cybered Westphalian Age." *Strategic Studies Quarterly* (Spring 2011): 32-61.

----------. "Uncivil and Post-Western Cyber Westphalia: Changing Interstate Power Relations of the Cybered Age." *The Cyber Defense Review*, Vol. 1, No. 1 (Spring 2016): 49-74.

----------. *Wars of Disruption and Resilience: Cybered Conflict, Power, and National Security*. Athens, GA: University of Georgia, 2011. Pp. 331.

Flynn, Matthew J. "Winning the Cyber War." *Journal of International Affairs*, January 29, 2018, https://jia.sipa.columbia.edu/online-articles/winning-cyber-war.

----------. "The Cyber 'Errand into the Wilderness': The 'Defending Forward' Inflection Point." *Georgetown Journal of International Affairs* Vol. 21 (Fall 2020): 71-79.

----------. "Civilians 'Defending Forward' in Cyberspace: Aligning Cyber Strategy and Cyber Operations." *The Cyber Defense Review* (Winter 2020): 29-39.

Giles, Keir with Andrew Monaghan. "Legality in Cyberspace: An Adversary View." The Letort Papers, Strategic Studies Institute. Carlisle, PA: United States Army War College Press, March 2014. Pp. 56.

Gray, Colin S. "Making Strategic Sense of Cyber Power: Why the Sky is not Falling." Carlisle, PA: Strategic Studies Institute and US Army War College Press, 2013. Pp. 67.
Iasiello, Emilio. "Fixing US National Cybersecurity: A Modest Proposal for Swallowing Pride and Reducing Egos." *Comparative Strategy*, Vol. 32, No. 4 (2013): 301-307.
Lewis, James A. "Conflict and Negotiation in Cyberspace." Center for Strategic and International Studies (CSIS), February 2013. Pp. 70.
Libicki, Martin. "Why Cyber War Should Not and Will Not Have Its Grand Strategist." *Strategic Studies Quarterly* (Spring 2014): 23-39.
Meyer, Paul. "Seizing the Diplomatic Initiative to Control Cyber Conflict." *The Washington Quarterly* (Summer 2015): 47-61.
Miller, Robert A., Daniel T. Kuehl and Irving Lachow. "Cyber War: Issue in Attack and Defense." *Joint Force Quarterly*, Issue 61, 2nd Quarter (2011): 18-23.
Murphy, Dennis M. "Attack or Defend: Leveraging Information and Balancing Risk in Cyberspace." *Military Review* (May-June 2010): 88-96.
Parker, Kevin L. LTCOL. "The Utility of Cyberpower." *Military Review* (May-June 2014): 26-33.
Saltzman, Ilai. "Cyber Posturing and the Offense-Defense Balance." *Contemporary Security Policy*, Vol. 34, No. 1 (2013): 40-63.
Stytz, Martin R. and Sheila B. Banks. "Toward Attaining Cyber Dominance." *Strategic Studies Quarterly* (Spring 2014): 55-87.
Wass de Czege, Huba. "Netwar: Winning in the Cyber Electromagnetic Dimension of 'Full Spectrum Operations.'" *Military Review* (March-April 2010): 20-32.
----------. "Warfare by Internet: the Logic of Strategic Deterrence, Defense, and Attack." *Military Review* (July-August 2010): 85-96.

**Cyber Operations**

Bonner, Lincoln E. "Cyber Power in 21st Century Joint Warfare." *Joint Force Quarterly,* Issue 74 (3rd Quarter 2014): 102-109.
Fink, Calle D., John D. Jordan, and James E. Wells. "Considerations for Offensive Cyber Operations." *Military Review* (May-June 2014): 4-11.
Hicks, J. Marcus. "A Theater-Level Perspective on Cyber." *Joint Force Quarterly*, Issue 76 (1st Quarter 2015): 58-63.
Kallberg, Jan and Bhavani Thuraisingham. "Cyber Operations: Bridging From Concept to Cyber Superiority." *Joint Force Quarterly*, Issue 68 (1st Quarter 2013): 53-58.
McGhee, James E. "Liberating Cyber Offense." *Strategic Studies Quarterly* (Winter 2016): 46-63.
Manzo, Vincent. "Deterrence and Escalation in Cross-Domain Operations: Where do Space and Cyberspace Fit?" *Joint Force Quarterly*, Issue 66 (3rd Quarterly 2012): 8-14.
Martin, William Jay and Emily Kaemmer. "Cyberspace Situational Understanding for Tactical Army Commanders." *Military Review* (July-August 2016): 18-24.
Rokke, Ervin J., Thomas A. Drohan, and Terry C. Pierce. "Combined Effects Power." *Joint Force Quarterly*, Issue 73 (2nd Quarter 2014): 26-31.
Williams, Brett T. "The Joint Force Commander's Guide to Cyberspace Operations." *Joint Force Quarterly,* Issue 73 (2nd Quarter 2014): 12-19.

***Russia and Estonia***

Brenner, Susan W. *Cyberthreats: The Emerging Fault Lines of the Nation State.* Oxford: Oxford University Press, 2009. Pp. 227.
Herzog, Stephen. "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses." *Journal of Strategic Security,* Vol. 4, No. 2, Summer 2011, Strategic Security in the Cyber Age: 49-60.
Laasme, Häly. "Estonia: Cyber Window into the Future of NATO." *Joint Force Quarterly,* Issue 63 (4th Quarter 2011): 58-63.
Russell, Alison Lawlor. *Cyber Blockades*. Washington DC: Georgetown University Press, 2014. Pp. 69-95.
Tikk, Eneken, Kadri Kaska, and Liis Vihul. *International Cyber Incidents: Legal Considerations.* Tallinn, Estonia: Cooperative Cyber Defence Centre of Excellence (CCDCOE), 2010. Pp. 132.

***Russo-Georgian Cyber War***

"Cyber Attacks Against Georgia: Legal Lessons Identified." Tallinn, Estonia: Cooperative Cyber Defence Centre of Excellence (CCDCOE), November 2008. Pp. 31.
Asmus, Ronald D. *A Little War That Shook the World: Georgia, Russia, and the Future of the West*. New York: Palgrave Macmillan, 2010. Pp. 272.
Cornell, Svante E. and S. Frederick Starr, Eds. *The Guns of August 2008: Russia's War in Georgia*. ME Sharpe, 2009. Pp. 279.
Hollis, David M. "Cyber War Case Study, Georgia 2008." *Small Wars Journal*. January 6, 2011. Pp. 10.
Karagiannis, Emmanuel. "The Russian Interventions in South Ossetia and Crimea Compared: Military Performance, Legitimacy, and Goals." *Contemporary Security Policy,* Vol. 35, No. 3 (2014): 400-420.
Korns, Stephen W. and Joshua E. Kastenberg. "Georgia's Cyber Left Hook." *Parameters* (Winter 2008-2009): 60-76.
Miller, Robert A. and Daniel T. Kuehl. "Cyberspace and the 'First Battle' in 21st-century War." *Defense Horizons,* Number 68 (September 2009), 1-6.
Russell, Alison Lawlor. *Cyber Blockades*. Washington DC: Georgetown University Press, 2014. Pp. 96-127.
Shakarian, Paulo. "The 2008 Russian Cyber Campaign Against Georgia." *Military Review* (November-December 2011): 63-68.

***Stuxnet***

*W32: Stuxnet Dossier*, *Symantec Security Response*. Symantec, Version 1.4, Nicholas Falliere. February 2011. Pp. 69.

Brown, Gary D. "Why Iran Didn't Admit Stuxnet Was an Attack." *Joint Force Quarterly,* Issue 63 (4th Quarter 2011): 70-73.
Lindsay, Jon R. "Stuxnet and the Limits of Cyber Warfare." *Security Studies,* Vol. 22, No. 3 (2013): 365-404.
Milevski, Lucas. "Stuxnet and Strategy: a Special Operation in Cyber Space?" *Joint Force Quarterly,* Issue 63 (4th Quarter 2011): 64-69.
Shakarian, Paul. "Stuxnet: Cyber Revolution in Military Affairs." *Small Wars Journal,* April 15, 2011. Pp. 10.

Zetter, Kim. *Countdown to Zero Day: Stuxnet and the Launch of the World First Digital Weapon*. New York: Crown Publishers, 2014. Pp. 433.

**Cyber Ideology (the Information War in Cyberspace)**

"Hacktivisim: Cyberspace has Become the New Medium for Political Voices." White Paper, McAfee. May 2012. Pp. 18.

Arquilla, John. "Cyberwar is Already Upon US: But Can it be Controlled?" *Foreign Policy Magazine,* February 27, 2012. Pp. 3.

---------- and David Ronfeldt. "Cyberwar is Coming!" *Comparative Strategy,* Vol. 12, No. 2 (Spring 1993): 141-165.

Bremmer, Ian. "Democracy in Cyber Space." *Foreign Affairs,* Vol. 89, Issue 6 (Nov-Dec 2010): 86-92.

Flynn, Matthew J. "Cyber Rebellions: The Online Struggle for Openness." *Journal of International Affairs*. Vol. 71, No. 1.5 (Special Issue: 2018): 107-114.

----------. "Strategic Cyber: Responding to Russian Online Information Warfare." *The Cyber Defense Review,* Special Edition, Cyber Conflict During Competition (2019): 193-207.

Libicki, Martin C. *Conquest in Cyberspace: National Security and Information Warfare*. New York, NY: Cambridge University Press, 2007. Pp. 323.

Rotberg, Robert I and Jenny C. Aker. "Mobile Phones: Uplifting Weak and Failed States." *The Washington Quarterly,* Vol. 36, No. 1 (2013): 111-125.

Tufekci, Zeynep. "Social Movements and Governments in the Digital Age: Evaluating a Complex Landscape." *Journal of International Affairs,* Vol. 68, No. 1 (Fall/Winter 2014): 1-18.

***China, the Great Firewall***

*China's Great Cannon*, The Citizen Lab, University of Toronto, April 2015.

Hachigian, Nina. "China's Cyber-Strategy." *Foreign Affairs* (March-April 2001): 118-133.

Lagerkvist, Johan. "New Media Entrepreneurs in China: Allies of the Party-State or Civil Society?" *Journal of International Affairs,* Vol. 65, No. 1 (Fall/Winter 2011): 169-182.

Zeng, Jinghan. "China's Date with Big Data: Will it Strengthen or Threaten Authoritarian Rule?" *International Affairs* Vol. 9, No. 6 (2016): 1443-1462.

and…

Baogang He. "Working With China to Promote Democracy." *The Washington Quarterly,* 36 (1) (Winter 2013): 37-53.

Sarotte, M.E. "China's Fear of Contagion: Tiananmen Square and the Power of the European Example." *International Security,* Vol. 37, No. 2 (Fall 2012): 156-182.

Yu Liu and Dingding Chen. "China Will Democratize." *The Washington Quarterly,* 35 (1) (Winter 2012): 41-63.

***The Arab Spring and Social Media***

"Civil Movements: The Impact of Facebook and Twitter." Dubai School of Government, *Arab Social Media Report,* 1(2) (May 2011): 1-30.

"New Media and Conflict after the Arab Spring." United States Institute of Peace, *Peaceworks* 80 (2012): 1-24.

Alterman, Jon. "The Revolution Will Not be Tweeted." *The Washington Quarterly,* 34 (4) (Fall 2011): 103-116.

Bachrach, Judy. "Wikihistory: Did the Leaks Inspire the Arab Spring?" *World Affairs* (July/Aug 2011): 35-44.

Doran, Michael S. "The Impact of New Media: The Revolution Will be Tweeted." In *The Arab Awakening: America and the Transformation of the Middle East,* Kevin Pollack, et al eds. Washington D.C.: Brookings Institute Press, 211. Pp. 369. (39-46).

Esseghaier, Mariam. "Tweeting Out a Tyrant:' Social Media and the Tunisian Revolution." *Wi Journal of Mobile Media,* Vol. 7, No. 1 (March 2013): 1-8.

Hussain, Muzammil M. "Digital Infrastructure Politics and Internet Freedom Stakeholders After the Arab Spring." *Journal of International Affairs,* Vol. 68, No. 1 (Fall/Winter 2014): 37-56.

Wheeler, Deborah. "The Internet and Youth Subculture in Kuwait." *Journal of Computer-Mediated Communication,* Vol. 8, Issue 2 (January 2003): online. [http://onlinelibrary.wiley.com/doi/10.1111/j.1083-6101.2003.tb00207.x/full]

----------, ed. *The Internet in the Middle East: Global Expectations and Local Imaginations in Kuwait.* Albany, NY: SUNY Press, 2006. Pp. 241. [same as above]

***Other, North Korea & Venezuela***

Baek, Jieun. "The Opening of the North Korean Mind: Pyongyang Versus the Digital Underground." *Foreign Affairs* (January-February 2017): 104-113.

Cha, Victor D. and Nicholas D. Anderson. "A North Korean Spring." *The Washington Quarterly,* Vol. 35, No. 1 (2012): 7-24.

Victoria, Gustavo Adolfo Vargas. "The Bolivarian Spring: What Are the Possibilities for Regime Change in Venezuela?" *Journal of International Affairs,* Vol. 68, No. 1 (Fall/Winter 2014): 269-283.

***ISIS, Online Terrorism***

Berger, J. M. and Jonathon Morgan. "The ISIS Twitter Census: Defining and Describing the Population of ISIS Supporters Online." The Brookings Project on US Relations with the Islamic World, Analysis Paper, No. 20, Center for Middle East Policy. Brookings Institute, March 2015. Pp. 67.

Vidino, Lorenzo and Seamus Hughes. "ISIS in America: From Retweets to RAQQA." Program on Extremism, George Washington University, December 2015. Pp. 50.

Benson, David C. "Why the Internet Is Not Increasing Terrorism." *Security Studies,* Vol. 23, No. 2 (2014): 293-328.

Brooks, Risa A. "Muslim 'Homegrown' Terrorism in the United States: How Serious is the Threat?" *International Security,* Vol. 36, No. 2 (Fall 2011): 7-47.

Cohen, Jared. "Digital Counterinsurgency: How to Marginalize the Islamic State Online." *Foreign Affairs* (November/December 2015): 52-58.

Ferguson, Micael P. "The Mission Command of Islamic State: Deconstructing the Myth of Lone Wolves in the Long Fight." *Military Review* (September-October 2017): 68-77.

Katagíri, Noriyuki. "ISIL, Insurgent Strategies for Statehood, and the Challenge for Security Studies." *Small Wars & Insurgencies*, Vol. 26, No. 3 (2015): 542-556.
Metz, Steven. "The Internet, New Media, and the Evolution of Insurgency." *Parameters*, Vol. XLII, No. 3 (Autumn 2012): 80-90.
Michael, George. "The New Media and the Rise of Exhortatory Terrorism." *Securities Studies Quarterly* (Spring 2013): 40-68.
Schultz, Robert William. "Countering Extremist Groups in Cyberspace." *Joint Force Quarterly*, Issue 79 (4th Quarter 2015): 54-56.
Sorenson, David S. "Confronting the Islamic State: Priming Strategic Communications: Countering the Appeal of ISIS." *Parameters*, Vol. 44, No. 3 (Autumn 2014): 25-36.
West, Allen B. "The Future of Warfare Against Islamic Jihadism: Engaging and Defeating Nonstate, Nonuniformed, Unlawful Enemy Combatants." *Military Review* (January-February 2016): 39-44.
Wood, Graeme. "What ISIS Really Wants." *The Atlantic*. March 2015: 1-43.

**China and Cyber War**

"APT 1, Exposing One of China's Cyber Espionage Units." Mandiant. February 2013. Pp. 76.
Krekel, Bryan, Patton Adams, and George Bakos. "Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage." Northrop Grumman Corp, Prepared for the US-China Economic and Security Review Commission, 7 March 2012. Pp. 137.

Austin, Greg. *Cyber Policy in China*. Polity, 2014. Pp. 203.
Bremer, Joel and Jon Lindsay. "Correspondence: Debating the Chinese Cyber Threat." *International Security*, Vol. 40, No. 1 (Summer 2015): 191-195.
Domingo, Francis C. "Conquering a New Domain: Explaining Great Power Competition in Cyberspace." *Comparative Strategy*, Vol. 35, No. 2 (2016): 154-168.
Gurmeet Kanwal, Gurmeet. "China's Emerging Cyber War Doctrine." *Journal of Defence Studies*, Vol. 3, No. 3 (July 2009): 14-22.
Hagestad, William T. *21st Century Chinese Cyberwarfare.* Ely, Cambridgeshire, UK: IT Governance Publishing, 2012. Pp. 314.
Li, Zhang. "A Chinese Perspective on Cyber War." *International Review of the Red Cross*, Vol. 94, No. 886 (Summer 2012): 801-807.
Lindsay, Jon R. "The Impact of China on Cybersecurity: Fiction and Friction." *International Security*, Vol. 39, No. 3 (Winter 2014-2015): 7-47.
----------, Tai Ming Cheung, and Derek S. Reveron, Eds. *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*. New York: Oxford University Press, 2015. Pp. 375.
Magnus Hjortdal, "China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence," *Journal of Strategic Security*, Vol. 4, No. 2 (2011): 1-24.
Manson, George Patterson. "Cyberwar: The United States and China Prepare for the Next Generation of Conflict." *Comparative Strategy*, Vol. 30, No. 2 (2011): 121-133.
Qiao, Liang and Wang Xiangsui. *Unrestricted Warfare: China's Master Plan to Destroy America*. Beijing: PLA Literature and Arts Publishing House, February 1999. Pp. 197.

Thomas, Tim L. *Decoding the Virtual Dragon.* Fort Leavenworth, KS: Foreign Military Studies Office, 2007. Pp. 352.
----------. *Dragon Bytes: Chinese Information-war Theory and Practice from 1995-2003.* Fort Leavenworth, KS: Foreign Military Studies Office, 2004. Pp. 168.
----------. "Google Confronts China's 'Three Warfares'." *Parameters* (Summer 2010): 101-113.

**Cyber Deterrence**

Betz, David. "Cyberpower in Strategic Affairs: Neither Unthinkable nor Blessed." *Journal of Strategic Studies,* Vol. 35, No. 5 (Oct 2012): 689-711.
Borghard Erica D. and Shawn N. Lonergan. "The Logic of Coercion in Cyberspace." *Security Studies* Vol. 26, No. 3 (2017): 452-481.
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.
Fischerkeller, Michael P. and Richard J. Harknett. "Deterrence is not a Credible Strategy for Cyberspace." *ORBIS* (Summer 2017): 381-393.
Gartzke, Erik and Jon R. Lindsay. "Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace." *Security Studies* 24, 2 (2015): 316-348.
Goodman, Will. "Cyber Deterrence: Tougher in Theory Than in Practice." *Strategic Studies Quarterly* (Fall 2010): 102-135.
Healey, Jason. "The Implications of Persistent (and Permanent) Engagement in Cyberspace." *Journal of Cybersecurity,* Vol. 5, Issue 1 (2019): online.
Leuprecht, Christian, Joseph Szeman, and David B. Skillicorn. "The Damoclean Sword of Offensive Cyber: Policy Uncertainty and Collective Insecurity." *Contemporary Security Policy* 40:3 (2019): 382-407.
Libicki, Martin C. "Cyberdeterrence and Cyberwar." RAND Corp, Prepared for the Air Force, 2009. Pp. 240.
Nakasone, Paul M. "A Cyber Force for Persistent Operations." *Joint Force Quarterly* 92 (1st Quarter 2019): 10-14.
Nye, Joseph S. "Deterrence and Dissuasion in Cyberspace." *International Security* Vol. 41, No. 63 (Winter 2016/2017): 44-71.
----------. "Is Deterrence Possible in Cyberspace?" Correspondence, Richard J. Harknett and Joseph Nye. *International Deterrence* Vol. 42, No. 2 (Fall 2017): 196-199.
----------. "Nuclear Lessons for Cyber Security?" *Strategic Studies Quarterly* (Winter 2011): 18-38.
Sharp, Travis. "Theorizing Cyber Coercion: The 2014 North Korean Operation Against Sony." *Journal of Strategic Studies* Vol. 40, No. 7 (2017): 898-926.
Smeets, Max. "The Strategic Promise of Offensive Cyber Operations." *Strategic Studies Quarterly,* Vol. 12, No. 3 (Fall 2018): 90-113.
Sterner, Eric. "Retaliatory Deterrence in Cyberspace." *Strategic Studies Quarterly* (Spring 2011): 62-80.
Stevens, Tim. "A Cyber War of Ideas: Deterrence and Norms in Cyberspace." *Contemporary Security Policy,* Vol. 33, No. 1 (April 2012): 148-170.
Valeriano, Brandon, Benjamin Jensen, and Ryan C. Maness. *Cyber Strategy: The Evolving Character of Power and Coercion.* New York, NY: Oxford University Press, 2018. Pp. 321.

---------- and Ryan C. Maness. *Cyber War Versus Cyber Realities: Cyber Conflict in the International System*. New York, NY: Oxford University Press, 2015. Pp. 266.

**Cyber as a Domain**

Barcomb, Kris E. "From Sea Power to Cyber Power: Learning from the Past to Craft a Strategy for the Future." *Joint Force Quarterly,* Issue 69 (2nd Quarter 2013): 78-83.

Dombrowski, Peter and Chris Demchak. "Cyber War, Cyber Conflict, and the Maritime Domain." *Naval War College Review*, Spring 2014, Vol. 67, No. 3: 71-96.

Healey, Jason. "Claiming the Lost Cyber Heritage." *Strategic Studies Quarterly* (Fall 2012): 11-19.

Lambeth, Benjamin S. "Airpower, Spacepower, and Cyberpower." *Joint Force Quarterly,* Issue 60 (1st Quarter 2011): 46-53.

Libicki, Martin C. "Cyberspace is Not a Warfighting Domain." *I/S: A Journal of Law and Policy,* Vol. 8, No. 2 (2012): 321-336.

Lynn, William J. III. "Defending a New Domain." *Foreign Affairs*, Vol. 89, Issue 5 (Sept-Oct 2010): 97-108.

Stavridis, James G. and Elton C. Parker. "Sailing the Cyber Ship." *Joint Force Quarterly*, Issue 65 (2nd Quarter 2012): 61-67.

**Norming Cyberspace**

Brantly, Aaron Franklin. "The Cyber Losers." *Democracy and Security,* 10, 2 (2014): 132-155.

Cerf, Vint, Patrick Ryan, and Max Senges. "Internet Governance is Our Shared Responsibility." *I/S: A Journal of Law and Policy for the Information Society,* Vol. 10, 1 (2014): 1-41.

Deibert, Ronald J. and Masashi Crete-Nishihata. "Global Governance and the Spread of Cyberspace Controls." *Global Governance*, 18, No. 3 (Jul-Sep 2012): 339-361.

----------. "The Road to Digital Unfreedom: Three Painful Truths About Social Media." *Journal of Democracy,* Vol. 30, No. 1 (Jan 2019): 25-39.

DeNardis, Laura. "Five Destabilizing Trends in Internet Governance." *I/S: A Journal of Law and Policy for the Information Society,* Vol. 12, No. 1 (2015): 113-133.

---------- and Mark Raymond. "The Internet of Things as a Global Policy Frontier." *US Davis Law Review,* Vol. 51, No. 2 (2017): 475-497.

Finnemore, Martha and Duncan B. Hollis. "Constructing Norms for Global Cybersecurity." *The American Journal of International Law,* Vol. 110, No. 3 (July 2016): 425-479.

Fleck, Dieter. "Searching for International Rules Applicable to Cyber Warfare – A Critical First Assessment of the New *Tallinn Manual*." *Journal of Conflict and Security Law*, Vol. 18, No. 2 (2013): 331-351.

Mueller, Milton. "Internet Security and Networked Governance in International Relations." *International Studies Review*, 15 (2013): 86-104.

----------. *Networks and States: The Global Politics of Internet Governance*. Cambridge, MA: MIT Press, 2010.

Raymond, Mark and Laura DeNardis. "Multistakeholderism: Anatomy of an Inchoate Global Institution. *International Theory*, 7, 3 (2015): 572-616.

Schmitt, Michael and Liis Vihul. "The Nature of International Law Cyber Norms." Tallinn Paper No. 5, CCDCOE, 2014. Pp. 1-31.

----------, Ed. *The Tallinn Manual on International Law Applicable to Cyber Warfare*. New York, NY: Cambridge University, 2013. Pp. 213.

Tikk-Ringas, EneKen. "International Cyber Norms Dialogue as an Exercise of Normative Power." *Georgetown Journal of International Affairs*, Vol XVII, No. III (Fall/Winter 2016): 47-59.

*This bibliography is compiled from scholarly literature. The topics covered reflect the priority of better understanding a cyber war. mjf*

Academic Journals

*Contemporary Security Policy (Routledge)*
*International Affairs (UK)*
*Journal of International Affairs (Columbia)*
*International Security (MIT)*
*Journal of Strategic Studies (Routledge)*
*Security Studies (Routledge)*
*The Washington Quarterly*
*World Politics (Cambridge)*
*Journal of Global Security Studies*

*Journal of Cybersecurity*
*Journal of Cyber Policy*
*Journal of Information Warfare*
*Journal of Cyber Conflict Studies*

Within PME Circles

*Joint Force Quarterly*
*Strategic Studies Quarterly*
*Parameters*
*Military Review*
*Small Wars Journal*