Cyber Conflict

Professor Robert Axelrod
axe@umich.edu

SPP 750.001, Winter 2014
TuTh 8:30-10, 1220 Weill Hall
Office Hours Tu 2-4

This course examines how cyberspace, particularly the Internet, can serve as a tool, target, and source of conflict for both state and non-state actors. Topics include: power in cyberspace, state control over cyberspace, methods of cyber conflict, laws and ethics of cyber conflict, cyber warfare, infrastructure threats and vulnerabilities, cyber deterrence and defense, and cyber conflict strategy and challenges.

The grading will be:

First Group Project	20%
Second Group Project	20%
Midterm Essay	15%
Take Home Final Exam due May 1	25%
Class Participation	20%

The required books are:

Singer, P. W. and Allan Friedman, 2014. Cybersecurity and Cyberwar (Oxford University Press).

Clarke, Richard and Robert K. Knake, 2010. Cyber War (New York: Harper Collins).

1. Introduction. Jan. 9

2. Technology. Jan. 14 and 16.

1. Nye, Joseph, 2011. Future of Power (NY: Public Affairs), pp. 126-45.
2. Singer and Friedman, pp.1-72.
3. Clark and Knake, 281-90. Skim.
4. "Cracked credibility; The NSA and cryptography," Economist, Sept. 17, 2013.
5. “Cloaks off; Spies and politics,” Economist, Nov. 2, 2013.
6. “A giant cage,” Economist, Apr. 6, 2013. (China)

3. The Internet As Battlespace. Jan. 21 and 23.

1. Clarke and Knake, pp. 1-32, and 69-101.

2. Axelrod, Robert and Rumen Iliev, "The Timing of Cyber Conflict," Proceedings of the National Academy of Sciences, forthcoming.

3. Rid, Thomas, "Cyberwar and Peace: Hacking Can Reduce Real-World Violence, Foreign Affairs, Nov./Dec. 2013, pp. 77-87.

4. Lewis, James Andrew, 2013. "Significant Cyber Incidents Since 2006." Center for Strategic and International Studies (skim).

4. Disruption and Attribution (and Russia, North Korea). Jan. 28 and 30.

1. Carr, Jeffrey, 2009. Inside Cyber Warfare (Sebastopol, CA: O'Reilly), pp. 89-90, 114-19, 161-71.

2. Rid, Thomas, 2013. Cyberwar Will Not Take Place (London: Hurst and Co.), pp.6-10.

3. "Lithuania Under Cyber Attack," Economist. June 1, 2013.

4. "Cyber-attack in the Czech Republic: Thieves in the Night, Economist, May 13, 2013.

5. Sobelman, Batsheva, "Israel braces as hackers launch Internet attack," LA Times, April 7, 2013.

6. Clayton, Mark, "In cyberarms race, North Korea emerging as a power, not a pushover," Christian Science Monitor, Oct. 19, 2013.

7. Perlez, Jane, "U.S. General Sees Hope for Chinese Help on Korea," NY Times, April 24, 2013. (last six paragraphs).

8. Singer and Friedman, pp. 72-76.

9. Boebert, W. Earl, "A Survey of Challenges in Attribution," in National Research Council**,** Proceedings of a Workshop on Deterring Cyberattacks, 2010, pp. 41-52.

10. Carr, Jeffrey, 2009. Inside Cyber Warfare (Sebastopol, CA: O'Reilly), 121-39.

11. "Haifa tunnel paralyzed by cyberattack, expert reveals," Haaretz, Oct. 27, 2013.

12. Wagensnell, Paul, "Cyberattack Against Israeli Highway System? Maybe Not," Tom's Guide US, Oct. 28, 2013.

5. China and Espionage. Feb. 4 and 6.

1. Lieberthal, Kenneth and Wang Jisi, "Addressing U.S.-China Strategic Distrust," March 30, 2012. Washington DC: Brookings Institution. Pp. vi-xiii and 1-50.

2. Ball, Desmond, 2011. "China's Cyber Warfare Capability," Security Challenges, vol. 7, pp. 81-103.

3. Singer and Friedman, pp. 91-96 and 138-144.

4. Sanger, David E. et al., “China's Army Is Seen as Tied to Hacking Against U.S.” NY Times, Feb. 19, 2013.

5. Rid, Thomas, 2013. Cyberwar Will Not Take Place (London: Hurst and Co.), ch 5 on Espionage, pp.81-112. (also relevant to Iran and attribution)

6. Clarke and Knake, 230-37.

6. Multi-faceted Conflict with Iran (Sanctions, Assassinations, Terrorism, Sabotage, Disruption, Espionage and Diplomacy). Feb. 11 and 13.

1. Langner, Ralph, “To Kill a Centrifuge: A Technical Analysis of What Stuxnet’s Creators Tried to Achieve,” (Arlington VA: The Langner Group), Nov. 2013. Pp. 3-23 and 36. Skim the rest.

2. Singer and Friedman, pp. 114-120. (Stuxnet including ethics)

3. Sanger, David E., 2012. Confront and Conceal: Obama’s Secret Wars and Surprising Use of American Power (NY: Crown), pp. 188-209 on Olympic Games including Stuxnet.

4. Rid, Thomas, 2013. Cyberwar Will Not Take Place (London: Hurst and Co.), pp. 26- 30 on DigiNotar hack.

5. Peterson, Scott, “Iran hijacked US drone, says Iranian engineer, Christian Science Monitor, Dec. 15, 2011.

6. Engel, Richard and Robert Windrem, NBC News, “Israel teams with terror group to kill Iran's nuclear scientists, U.S. officials tell NBC News,” Feb. 9 2012.

7. “Mojtaba Ahmadi, Iranian Revolutionary Guard Working on Cyber Warfare, Killed in Possible Assassination,” Huff Post, Oct 3, 2013.

8. Kulish, Nicolas and Jodi Rudoren, “Plots Are Tied to Shadow War of Israel and Iran,” New York Times, August 8, 2012.

7. U.S. Cyber Organization and Policy. Feb. 18 and 20.

1.Clark and Knake, pp. 33-68.

2. Shane, Scott, ‘New Leaked Document Outlines U.S. Spending on Intelligence Agencies,” NY Times, August 29, 2013.

3. Libicki, Martin, 2012. Crisis Escalation in Cyberspace (Santa Monica, CA: Rand), pp. 114-21.

4. Fuerth, Leon, “Cyberpower from the Presidential Perspective,” in Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (eds.), Cyberpower and National Security (Washington, DC: National Defense University Press), pp. 557-563.

5. Singer and Friedman, pp. 133-138

6. Greenwald, Glenn and Ewen MacAskill, “Obama orders US to draw up overseas target list for cyber-attacks,” Guardian, June 7, 2013.

7. Presidential Policy Directive 20, “U.S. Cyber Operations Policy,” November 16, 2012.

8. Singer and Friedman, pp. 162-65.

9. "Hiring digital 007s; Consultancies and spy chiefs" Economist, June 15, 2013.

10. Carr, Jeffrey, 2009. Inside Cyber Warfare (Sebastopol, CA: O'Reilly), pp. 176-77.

11. Savage, Charlie, "Judge Questions Legality of N.S.A.Phone Records," NY Times, Dec. 16, 2013.

8. Cyber War. Feb. 25 and 27.

1. Rattray, Gregory and Jason Healey, "Categorizing and Understanding Cyber Capabilities and Their Use," in National Research Council**,** Proceedings of a Workshop on Deterring Cyberattacks (2010), pp. 77-97.

2. Singer and Friedman, pp. 120-133.

3. Liff, Adam P., 2011. "Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War," Journal of Strategic Studies, vol. 35, pp. 401-28.

4. Sanker, Tim, "Pentagon Is Updating Conflict Rules in Cyberspace," New York Times, June 27, 2013.

5. Mueller, John, 2009. "War Has Almost Ceased to Exist," Political Science Quarterly, vol. 124, pp. 297-231.

6. Clark and Knake, 144-78.

9. Defense and Security. March 11 and 13.

1. Clark and Knake, pp. 103-44.

2. Singer and Friedman, pp. 166-180 and 205-246

3. Drew, Christopher, "Stolen Data Is Tracked to Hacking at Lockheed," New York Times, June 3, 2011.

4. Axelrod, Robert and Larissa Forster, "Interpersonal Aspects of Cyber Security," Unpublished May 13, 2013.

5. Hosenball, Mark, and Warren Strobel, "Exclusive: Snowden persuaded other NSA workers to give up passwords – sources," Reuters, Nov. 7, 2013.

6. Carr, Jeffrey, 2009. Inside Cyber Warfare (Sebastopol, CA: O'Reilly), pp. 179-89.

10. Deterrence and Crisis Stability. March 18 and 20.

1. Clarke and Knake, pp. 179-218.

2. Singer and Friedman, pp. 144-61.

3. Libicki, Martin, "Pulling Punches in Cyberspace," in National Research Council**,** Proceedings of a Workshop on Deterring Cyberattacks (2010), pp. 123-147.

4. Libicki, Martin, 2012. Crisis Escalation in Cyberspace (Santa Monica, CA: Rand), pp. 99-114.

5. Lukasik, Stephen, J., “A Framework for Thinking About Cyber Conflict and Cyber Deterrence with Possible Declaratory Policies for These Domains,” in National Research Council**,** Proceedings of a Workshop on Deterring Cyberattacks (2010), pp. 99-121.

11. Non-State Actors. March 25 and 27.

1. Singer and Friedman, pp. 96-106. (Cyberterrorists)

2. Rid, Thomas, 2013. Cyberwar Will Not Take Place (London: Hurst and Co.), pp. 113-38. (Subversives, Hactivists)

3. Singer and Friedman, pp. 77-84. (Hactivists)

4. Singer and Friedman, pp. 106-114. (Dissidents and Patriots)

5. Singer and Friedman, pp. 85-91. (Criminals)

6. Wilson, Clay, “Cyber Crime,” in Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (eds.), Cyberpower and National Security, 2009. (Washington, DC: National Defense University Press), pp. 415-36.

7. “The Next Generation of Cybercrime: How It’s Evolved, Where It’s Going,” SecureWorks, 2010, 3-11.

8. Menn, Joseph, “Special Report - U.S. cyberwar strategy stokes fear of blowback,” Reuters, May 10, 2013. (Buyers of Zero-Day Exploits)

12. Governance, and Law. April 1 and 3.

1. Singer and Friedman, pp. 180-204.

2. Clarke and Knake, 219-255.

3. Schmitt, Michael, N., “Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense, and Armed Conflicts,” in National Research Council**,** Proceedings of a Workshop on Deterring Cyberattacks, 2010. pp. 151-78

13. Ethics, Norms and Negotiations. April 8 and 10.

1. Belk, Robert and Matthew Noyes, 2012. On the Use of Offensive Cyber Capabilities (JFK School of Government), pp. 75-110.

2. Farnsworth, Timothy, “China and Russia Submit Cyber Proposal,” Arms Control Today, 2011, pp. 35-36.

3. Steinbrunner, John, ”Prospects for Global Restraint on Cyberattack,” Arms Control Today, 2011, pp. 21-26.

4. Lieberthal, Kenneth and Peter W. Singer. 2012. "Cybersecurity and U.S.-China Relations." Brookings Institution, 1-33.

5. Ramo, Joshua, “Talking Cyberthreats with China” NY Times, July 9, 2013.

6. Carr, Jeffrey, 2009. Inside Cyber Warfare (Sebastopol, CA: O’Reilly Press, 2009). pp. 161-178.

14. Future of the Internet and Cyber Conflict. April 15 and 17.

1. Clarke and Knake, 257-79.
2. Singer and Friedman, pp. 247-56.

15. Review. April 22.

Final Exam Due May 1.