Introduction to Cyberconflict

Wednesday, 9:00-10:40 | Online

2021 Winter Term

Professor: Cameran Ashraf, Ph.D.
Email: AshrafC@spp.ceu.edu
Office: Online
Office Hours: TBA

Course Description

The Internet is the dominant communications medium of the 21st century, facilitating open communications across the world and simultaneously representing a strategic threat and opportunity for conflict. Across the globe states have extended and expanded military and espionage actions in cyberspace to ensure protection of strategic domestic assets as well as to target desired foreign assets in furtherance of military, political, and security objectives. Through case study analysis and examination of relevant literature, including considering the definitional ambiguity of "cyberconflict", this course will chart the history and evolution of the Internet as a theater of combat operations and a space of strategic military importance. Broader social implications of the militarization of the Internet and the role of non-state actors will also be discussed.

Course Texts

All course texts will be posted on the class website. Students are strongly encouraged to download and print out the readings instead of reading from their computers. Reading a physical copy contributes to superior comprehension. Printing out copies of the readings can be done at the computer labs or the SPP main office.

Course Structure

This course is designed as a student-centric graduate seminar. There is no hand-holding. What you get out of this class will be precisely what you put into it.

Assignments - <u>Please note that all papers will be submitted through the TurnItIn system!</u>

<u>Discussion & Forum Participation</u>

This course has a strong participation component, and you are expected to discuss the readings, films, lectures, and class comments at every class meeting. If you are uncomfortable doing this, please consider dropping the course as it is an important component of your grade.

An important part of the course grade consists of weekly class web forum participation. Students must post at minimum one question or comment per week related to the readings or news events related to the class. Ideally this will be something you are interested in discussing during class. These must be posted to the forums by 12 PM the day before class. Posts which are late will be marked as a zero.

Papers

This course has multiple options for your term papers. This is designed to give students flexibility in approaching the subject in a way which will benefit their academic and professional goals. You will either do a separate policy brief and choose to do a media or personal data analysis paper OR you will submit a combined policy brief and media or personal data analysis paper. Please note that for all papers you are allowed to go over the wordcount.

CHOOSE ONE:

Media Analysis (1,250 words)

Policy is influenced by media, art, and culture. You will be expected to prepare a short media analysis and analyze some aspect of media (movie, books, video game, poetry, photography, etc.!) from a critical standpoint. This analysis will discuss the broader themes from the angle of class lecture, discussion, readings, and how they fit in with public policy. For instance: how is policy represented in the chosen media? How can the chosen media influence policy?

Personal Data Analysis (1,250 words)

Personal data has become increasingly weaponized as states seek to destabilize other states through targeted advertising and disinformation on social media. For this assignment you'll download your social media data and analyze it.

Once you've looked through your data, you'll examine it to see how accurate it reflects who you are. For example, my Twitter data says I'm interested in women's cosmetics, which I am not, but also that I'm interested in Books and Literature, which I am. In your analysis you'll be looking to address some of the following questions:

1) How accurate is your data profile? Were there any surprises?
2) How could a foreign power utilize this data as part of a disinformation campaign?
3) How can you balance a private social media company's need for profit versus its social obligations?
4) Now that you've seen your data and know what it looks like, from a cybersecurity perspective how should a) policymakers, b) civil society, c) governments, and d) individuals engage with this "brave new world" of big personal data?

In addition, your paper should include at least one policy recommendation and discussion related to your findings.

REQUIRED:

Policy Brief (1,250 words)

Students will be expected to prepare a policy brief on a course topic of their choice, approved by the professor. This paper will take some aspect of the course subject and provide a policy brief on the issue with recommendations. Students will be expected to provide a brief background of the topic, discuss the current policy situation, discuss policy options, provide 1-3 recommendations, and discuss the potential outcomes of their recommendations including benefits and how their proposals might not work as intended.

OPTIONAL:

Combined Paper (2,400 words – a 100 word discount!)

Can be done INSTEAD of separate media/personal data analysis and policy brief. Instead of a policy brief AND media analysis, students can opt to **combine** both the policy brief and personal data/media analysis into one paper. This paper would integrate media or reflections on their personal data into a policy brief to provide a more substantial discussion of a course-related related topic. For example, students can examine one of the movies we watched, demonstrate how policy was implemented in the film, and then use that as a basis for developing a new policy moving forward in greater depth. Alternatively, they can examine their personal data, look at the specific ways in which that data could be weaponized (maybe based on gender, nationality, etc.) and discuss policy recommendations from that perspective.

Simulation

One day of class is reserved for a cybersecurity simulation that will divide the class into two teams. More details on this assignment will be distributed to class later in the term.

Films:

This is a list of approved films for your film review. Some may be shown in class, and further films may be approved. You will be notified either via email or on the course website of new approved films. If there are additional films which you feel may be relevant, please discuss with the professor!

We Are Legion: The Story of the Hacktivists
The Perfect Weapon
Sneakers
WarGames
We Steal Secrets
The Fifth Estate
Zero Days
Snowden
The Great Hack

Class Policies

- All university policies relating to plagiarism, cheating, harassment, etc. will be fully enforced.
- Late papers without a valid written excuse lose 10% of their grade per day after the deadline.
- SPP policy is to fail students with more than one unexcused absence for a 2-credit course and more than two unexcused absences for a 4-credit course. Alternatively, final grades may be lowered in proportion to unexcused absences.
- Be respectful to other students and to yourself.
- I am an understanding individual. If there are things happening in your life which may prevent you from being successful in class, please come speak with me. I am on your side.
- The instructor reserves the right to change this syllabus at any time.

Breakdown of final grade by assignments:

Policy Paper =	**35%**
Media Analysis =	**30%**
Class Discussion =	**15%**
Simulation =	**10%**
Forum Participation =	**10%**

Reading Schedule

The following reading schedule is subject to change. Students will be held responsible only for those readings posted on the class website. Normally these will be posted at least a week in advance.

Week 1 (Jan. 13): Introduction

Class introductions, course outline.

Week 2 (Jan. 20): Surveying the Landscape

Blinder, A., & Perlroth, N. (2018, September 26). A Cyberattack Hobbles Atlanta, and Security Experts Shudder. The New York Times. Retrieved from https://www.nytimes.com/2018/03/27/us/cyberattack-atlanta-ransomware.html

Mazzetti, M., Perlroth, N., & Bergman, R. (2019, December 22). It Seemed Like a Popular Chat App. It's Secretly a Spy Tool. The New York Times. Retrieved from https://www.nytimes.com/2019/12/22/us/politics/totok-app-uae.html

Sanger, D. E., & Broad, W. J. (2017). Trump Inherits a Secret Cyberwar Against North Korean Missiles. *New York Times*, *4*.

Sanger, D. E., & D. (2017, October 15). The World Once Laughed at North Korean Cyberpower. No More. Retrieved from https://www.nytimes.com/2017/10/15/world/asia/north-korea-hacking-cyber-sony.html

Strick, Benjamin. (2020). "West Papua: New Online Influence Operation Attempts to Sway Independence Debate." Bellingcat. https://www.bellingcat.com/news/2020/11/11/west-papua-new-online-influence-operation-attempts-to-sway-independence-debate/.

Zetter, K. (2016). Inside the cunning, unprecedented hack of Ukraine's power grid. *WIRED, March*, *3*, 2016.

Week 3 (Jan. 27): What is Cyberwar?

Antolin-Jenkins, V. M. (2005). Defining the parameters of cyberwar operations: looking for law in all the wrong places. *Naval L. Rev.*, *51*, 132.

Greenberg, A. (2019, August 23). Cyberwar: The Complete Guide. Wired. Retrieved from https://www.wired.com/story/cyberwar-guide/

Klimburg, A. (2011). Mobilising cyber power. *Survival*, *53*(1), 41-60.

Manjikian, M. M. (2010). From global village to virtual battlespace: The colonizing of the internet and the extension of realpolitik. *International Studies Quarterly*, *54*(2), 381-401.

Rid, T. 2012. Cyber war will not take place. *Journal of Strategic Studies* 35 (1):5–32.

Sanders, C. M. (2018). The Battlefield of Tomorrow, Today: Can a Cyberattack Ever Rise to an Act of War Note. Utah Law Review, 2018(2), i–522.

Stone, J. 2013. Cyber War Will Take Place! *Journal of Strategic Studies* 36 (1):101–108.

Warner, M. 2012. Cybersecurity: a pre-history. *Intelligence and National Security* 27 (5):781–799.

Whetham, D. (2016). Cyber Chevauchees: Cyber war can happen. Binary Bullets: The Ethics of Cyberwarfare, 75–88.

OPTIONAL: Beidleman, S. W. 2009. *Defining and deterring cyber war*. DTIC Document.

Week 4 (Feb. 3): Movie & Discussion

Week 5 (Feb. 10): Methods and Tactics

Andress, J., & Winterfeld, S. (2013). Cyber Threatscape. In Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners (2 edition). Amsterdam ; Boston: Syngress.

Baram, G., & Lim, K. (2020, June 5). Israel and Iran Just Showed Us the Future of Cyberwar With Their Unusual Attacks. Foreign Policy.

Blank, Stephen. "Cyber War and Information War à la Russe." (2017).

Greenberg, A. (2020, October 23). How 30 Lines of Code Blew Up a 27-Ton Generator. Wired.

Jensen, B., Valeriano, B., & Maness, R. (2019). Fancy bears and digital trolls: Cyber strategy with a Russian twist. Journal of Strategic Studies, 42(2), 212–234.

Warf, B., & Fekete, E. (2015). Relational geographies of cyberterrorism and cyberwar. *Space and Polity*, 1-15.

Wheeler, T. (2018, September 12). In Cyberwar, There are No Rules. Foreign Policy. Retrieved January 8, 2019, from https://foreignpolicy.com/2018/09/12/in-cyberwar-there-are-no-rules-cybersecurity-war-defense/

Week 6 (Feb. 17): Case Study: Russian Operations 2007-Present

Movie: Operation Infektion

Alba, D., & Frenkel, S. (2019, October 30). Russia Tests New Disinformation Tactics in Africa to Expand Influence. The New York Times. Retrieved from https://www.nytimes.com/2019/10/30/technology/russia-facebook-disinformation-africa.html

Evron, G. 2008. Battling botnets and online mobs: Estonia's defense efforts during the internet war. *Geo. J. Int'l Aff.* 9:121.

Greenberg, Andy. 2018. "The Untold Story of NotPetya, the Most Devastating Cyberattack in History." Wired, August 22, 2018.

Harris, S., Lubold, G., & Sonne, P. (2018, January 05). How Kaspersky's Software Fell Under Suspicion of Spying on America. Retrieved from https://www.wsj.com/articles/how-kasperskys-software-fell-under-suspicion-of-spying-on-america-1515168888

Korns, S. W., & Kastenberg, J. E. (2009). *Georgia's cyber left hook*. ARMY WAR COLLEGE CARLISLE BARRACKS PA STRATEGIC STUDIES INSTITUTE.

Wentworth, T. 2008. How Russia May Have Attacked Georgia's Internet. *Newsweek.* http://www.newsweek.com/how-russia-may-have-attacked-georgias-internet-88111

Wirtz, J. (2015). 'Cyber War and Strategic Culture: The Russian Integration of Cyber Power into Grand Strategy' in *Cyber war in perspective: Russian aggression against Ukraine*. Tallinn: CCDCOE.

OPTIONAL: Lewis, J. (2015). 'Compelling Opponents to Our Will': The Role of Cyber Warfare in Ukraine in *Cyber war in perspective: Russian aggression against Ukraine*. Tallinn: CCDCOE.

Week 7 (Feb. 24): Case Study: Stuxnet

Gross, M. J. (2011). A declaration of cyber-war. *Vanity Fair*, *53*(4).

Gross, M. J. (2013). Silent War. *Vanity Fair*, (July).

Zetter, K. (2011). How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History. *WIRED*. Retrieved from https://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/

Zetter, K. (2014). An unprecedented look at Stuxnet, the world's first digital weapon. *Wired. com. November*, *3*, 14.

Zetter, Kim, and Huib Modderkolk. (2019). "Revealed: How a Secret Dutch Mole Aided the U.S.-Israeli Stuxnet Cyberattack on Iran." Yahoo News. September 2, 2019.

Week 8 (Mar. 3): Information and Disinformation

Higgins, A., McIntire, M., & Dance, G. J. x. (2017, December 22). Inside a Fake News Sausage Factory: 'This Is All About Income.' The New York Times.

Marwick, A., & Lewis, R. (2017). Media manipulation and disinformation online. New York: Data & Society Research Institute.

Nimmo, B. (2015, May 19). Anatomy of an Info-War: How Russia's Propaganda Machine Works, and How to Counter It. Retrieved January 8, 2019, from https://www.stopfake.org/en/anatomy-of-an-info-war-how-russia-s-propaganda-machine-works-and-how-to-counter-it/

Polyakova, C. M. and A. (2018, May 25). The West is ill-prepared for the wave of "deep fakes" that artificial intelligence could unleash. Brookings Institute. Retrieved January 8, 2019, from https://www.brookings.edu/blog/order-from-chaos/2018/05/25/the-west-is-ill-prepared-for-the-wave-of-deep-fakes-that-artificial-intelligence-could-unleash/

Rid, T. (2016, October 20). How Russia Pulled Off the Biggest Election Hack in U.S. History. Esquire Magazine. Retrieved January 8, 2019, from https://www.esquire.com/news-politics/a49791/russian-dnc-emails-hacked/

Susskind, J. (2018, December 4). Opinion | Chatbots Are a Danger to Democracy. The New York Times. Retrieved from https://www.nytimes.com/2018/12/04/opinion/chatbots-ai-democracy-free-speech.html

OPTIONAL: Koh, Y., & Wells, G. (2018, December 13). The Making of a Computer-Generated Influencer. Wall Street Journal. Retrieved from https://www.wsj.com/articles/the-making-of-a-computer-generated-influencer-11544702401

Week 9 (Mar. 10): Movie & Discussion

Week 10 (Mar. 17): Global Cybersecurity Challenges

Baezner, M. (2018). *Regional rivalry between India-Pakistan: Tit-for-tat in cyberspace*. ETH Zurich.

Ben-Hassine, W., & Samaro, D. (2019). Restricting cybersecurity, violating human rights: Cybercrime laws in MENA region. OpenGlobalRights. https://www.openglobalrights.org/restricting-cybersecurity-violating-human-rights/

Calderaro, A., & Craig, A. J. S. (2020). Transnational governance of cybersecurity: Policy challenges and global inequalities in cyber capacity building. Third World Quarterly, 41(6), 917–938. https://doi.org/10.1080/01436597.2020.1729729

Kshetri, N. (2019). Cybercrime and Cybersecurity in Africa. Journal of Global Information Technology Management, 22(2), 77–81. https://doi.org/10.1080/1097198X.2019.1603527

Schaake, M. (2020, October 19). The Lawless Realm. Foreign Affairs, November/December 2020. https://www.foreignaffairs.com/articles/world/2020-10-13/lawless-realm

Week 11 (Mar. 24): Global Cybersecurity Challenges II

Consumer Tech and the future of Cybersecurity:
European Commission. 2019. "EU Coordinated Risk Assessment of the Cybersecurity of 5G Networks." European Union.

International Humanitarian Law and Cyberconflict:
Gisel, L., Rodenhäuser, T., & Dörmann, K. (2020). Twenty years on: International humanitarian law and the protection of civilians against the effects of cyber operations during armed conflicts. *International Review of the Red Cross*, 1–48.

Non-state actors and Cyberconflict:
Mazzetti, M., Goldman, A., Bergman, R., & Perlroth, N. (2019, March 21). A New Age of Warfare: How Internet Mercenaries Do Battle for Authoritarian Governments. The New York Times.

The Human Element:
McDermott, R. (2019). Some emotional considerations in cyber conflict. Journal of Cyber Policy, 4(3), 309–325. https://doi.org/10.1080/23738871.2019.1701692

Nakashima, Ellen, and Greg Bensinger. 2019. "Former Twitter Employees Charged with Spying for Saudi Arabia by Digging into the Accounts of Kingdom Critics." Washington Post. November 6, 2019.

Week 12 (Mar. 31): The Future

Alba, Davey. 2019. "Facebook Discovers Fakes That Show Evolution of Disinformation." The New York Times, December 20, 2019, sec. Business.

Citron, D., & Chesney, R. (2020, June 29). Deepfakes and the New Disinformation War. January/February 2019. https://www.foreignaffairs.com/articles/world/2018-12-11/deepfakes-and-new-disinformation-war

Fryer-Biggs, Zachary. (2019). "Coming Soon to a Battlefield: Robots That Can Kill." The Atlantic, September 3, 2019.

Klincewicz, M. (2015). Autonomous Weapons Systems, the Frame Problem and Computer Security. Journal of Military Ethics, 14(2), 162-176

Markoff, J. (2014). Fearing bombs that can pick whom to kill. *New York Times*, *11*.

Pasquale, F. (2020, October 15). 'Machines set loose to slaughter': The dangerous rise of military AI. The Guardian. https://www.theguardian.com/news/2020/oct/15/dangerous-rise-of-military-ai-drone-swarm-autonomous-weapons

Simonite, T. (2013, February 13). Welcome to the Malware-Industrial Complex. Retrieved March 3, 2014, from MIT Technology Review

Weinstein, James Stavridis, Dave. 2016. “The Internet of Things Is a Cyberwar Nightmare.” Foreign Policy (blog). November 3, 2016.

OPTIONAL: Docherty, B. (2012). *Losing humanity: The case against killer robots*.

OPTIONAL: Topol, S. (2016). Killer Robots Are Coming And These People Are Trying To Stop Them. *BuzzFeed*. Retrieved from https://www.buzzfeed.com/sarahatopol/how-to-save-mankind-from-the-new-breed-of-killer-robots

OPTIONAL: Chesney, R., & Citron, D. K. (2018). Deep fakes: a looming challenge for privacy, democracy, and national security.