Example Course Syllabus

POLSCI/PUBPOL XXX: Internet, Social Media & Conflict

Fall 2020 Syllabus

Instructor: Nadiya Kostyuk	**Office:**
Instructor's Office Hours:	**E-mail:** nadiya@umich.edu
Classroom:	**Meeting Times:**

Course description: This course focuses on the various ways in which the Internet affects conflict. After introducing students to the major theoretical and policy debates regarding the Internet's effects on politics, this course will go on to investigate the domestic and international consequences of these effects. On the domestic front, the course focuses on ways that the Internet and social media drive the prevention, onset, duration, and intensity of violent and non-violence conflicts between a state and its citizens. Topics include censorship, surveillance, propaganda campaigns, and network disruptions. On the international front, the course examines how cyber conflict unfolds between states. The course concludes by investigating how struggles for supranational control of cyberspace are affecting interstate relations and, more generally, international order.

Objectives: The key objectives of this course are to equip students with tools to help them:

- understand current state-of-the-art research and developments on the topic of the Internet, social media, and conflict;
- critically evaluate the fast-moving debates and empirical research being produced on this topic;
- reflect on and develop their own understanding of how state attempts to control cyberspace are changing both domestic and international politics;
- conduct rigorous empirical research on this topic;
- derive actionable policy recommendations and communicate those recommendations to both specialist and non-specialist audiences.

Prerequisites: No prerequisite classes are required.

Grading and Assignments

Grades will be based on weekly attendance and participation (20%), a written discussion summary (10%), a policy memo (10%), participation in a war-game exercise (10%), and a team after-action report from the exercise (30%).

(1) **Classroom participation** (20%). Students are expected to engage fully the readings and to actively participate in all discussions and debates. To achieve a high participation grade, students should contribute to in-class discussions through active listening and by advancing the conversation and providing constructive feedback (e.g., on in-class presentations) when prompted to do so.

(2) **Written discussion summary** (10%). Students are to prepare a 400- to 500-word critical summary of one the required readings. In this summary, the student should identify the reading's main question, its main argument, the method/s the author uses to answer the research question, the main findings, and whether the student finds the argument and analysis convincing. In addition, students should mention any parts of the reading that they did not understand. Please note that not all required readings will include full-fledged empirical analyses. In the absence of such, students should explain what evidence the author uses to support the argument. The summary is **due on the morning of the class meeting during which we will discuss the work in question**.

(3) **Policy memo** (10%). Students are to prepare a 1,500-word (max.) policy memo that summarizes the current state of scientific knowledge on either the Internet or social media regarding a particular aspect of conflict (e.g., its prevention, onset, intensity, or duration). Students should conclude their memos by formulating basic policy recommendations. We will discuss how to formulate policy recommendations in detail in class. The memo is **due at the beginning of the Week 9 class meetings**.

(4) **War-game exercise** (10%). **During Week 12**, students will participate in a war-game exercise. Assigned various roles in the U.S. government, students, grouped into teams, will be tasked with devising a set of policy responses to a cyber-threat. Students will be graded based on their individual contributions to this exercise. We will discuss the specifics of the war game in detail in class.

(5) **Team after-action report** (30%). **During Week 13**, the students will spend some time working on a team after-action report in class. This report should include the following sections: (1) a description of the war game; (2) a set of suggested policy recommendations and their feasibility; (3) benefits and challenges of working in

a team responsible for dealing with a cyber threat; (4) lessons learned from working on this scenario; and (5) improvements that could be made at the future version of this war game. We will discuss the specific details of this after-action report in class.

Late assignment submissions: Grades will be reduced by one-letter grade per day that an assignment is late; alternative arrangements will be made only for excused absences, such as for medical and family emergencies.

Grading and grade-grievance policy: Good grades will be awarded for work that is completed fully, rigorously, and insightfully. I will strive to provide constructive feedback on assignments. Any grievances must be submitted in writing after a 48-hour waiting and review period.

Literature in assignments:

- Due to the topic's novelty, much of the cutting-edge research has not yet been officially published in academic outlets. Students should feel free to use a variety of sources — e.g., academic articles, books, working papers, news sources, and reports by NGOs, governments, and think tanks. Regardless of the source, students are responsible for critically evaluating the content they cite.

- To improve the rigor of their analyses, I expect students to cite underrepresented voices, paying attention to the gender and geographic balance of their citations.

Course Policies

Student Mental Health and Well-Being: University of Michigan is committed to advancing the mental health and well-being of its students. If you or someone you know is feeling overwhelmed, depressed, and/or in need of support, services are available. For help, contact Counseling and Psychological Services (CAPS) at (734) 764-8312 and https://caps.umich.edu/ during and after hours, on weekends and holidays, or through its counselors physically located in schools on both North and Central Campus. You may also consult University Health Service (UHS) at (734) 764-8320 and https://www.uhs.umich.edu/mentalhealthsvcs, or for alcohol or drug concerns, see https://www.uhs.umich.edu/ aodresources. For a listing of other mental health resources available on and off campus, visit: http://umich.edu/ mhealth/.

Learning needs: All students with special needs requiring accommodations should present the appropriate paperwork from the Service for Students with Disabilities. For more information, see https://ssd.umich.edu/. It is the student's responsibility to present this paperwork in a timely fashion and follow up with the instructor about the accommodations being offered.

Discrimination & Harassment: "The University of Michigan has, as one of its core values, an abiding commitment to sustaining a community in which the dignity of every individual is respected. Key to this value are efforts to foster and nurture an environment of civility and mutual respect by preventing discrimination and harassment on our campus." For a list of prohibited forms of discrimination and harassment, as well as resources about where to get help, please see http://www.hr.umich.edu/oie/cc/about.html.

Religious Holidays: Those students who observe a university-recognized religious holiday on a section day should contact me within the **first two weeks** in order to receive an excused absence.

Attendance: Regular attendance is expected, as is full engagement in classwork activities. Please arrive on time, turn off your cell phone, and stay for the entire class period.

Classroom Courtesy: Our goal is to become attentive listeners as well as critical thinkers and eloquent speakers. It is perfectly acceptable to disagree with other students, but all responses should be directed toward the content of their ideas rather than at their individual identities. Moreover, remember that private conversations or disrespectful comments hinder your learning and the learning of others.

Academic Dishonesty, Cheating, and Plagiarism: Academic dishonesty, cheating, and plagiarism of any kind are unacceptable. There are no exceptions. Instructors will follow University of Michigan procedures when there is sufficient evidence of plagiarism. For details, see http://www.lib.umich.edu/academicintegrity/understanding-plagiarism-and-academic-integrity.

Writing Help: This course requires basic academic writing skills. If you need help with your writing at any point, or if English is not your first language and you feel that you need additional support, I recommend contacting the Sweetland Writing Center (1139 Angell Hall, 764-0429, http://www.lsa.umich.edu/sweetland/).

General Readings

There are no general required readings, but if you are interested in getting acquainted with the topic, the following books are a useful place to start:

- DeNardis, Laura. *The Global War for Internet Governance.* Yale University Press, 2014.
- Zetter, Kim (2014). *Countdown to Zero Day: Stuxnet and the launch of the world's first digital weapon.* Broadway books.
- Weidmann, Nils B., and Espen Geelmuyden Rød. *The Internet and Political Protest in Autocracies.* Oxford Studies in Digital Politics, 2019.
- Deibert, R., Palfrey, J., Rohozinski, R., & Zittrain, J. (2011). *Access Contested: Security, identity, and resistance in Asian cyberspace.* MIT Press.
- Roberts, Margaret E. (2018) *Censored: Distraction and diversion inside China's Great Firewall.* Princeton University Press.

Section Overview

Section	Section Date	Section Title
1	09/08/2020	Introduction, the Internet
2	09/15/2020	Internet and politics
3	09/22/2020	Why control the Internet?
4	09/29/2020	Concepts and theories of cyberattacks
5	10/06/2020	Conflict prevention: censorship and net restrictions (domestic)
6	10/14/2020	Conflict prevention: deterrence (foreign)
7	10/20/2020	Conflict onset (domestic)
8	10/27/2020	Conflict onset (foreign)
9	11/03/2020	Conflict intensity and duration (domestic) **Policy Memo due at the beginning of class**
10	11/10/2020	Conflict intensity and duration (foreign)
11	11/17/2020	Future of the Internet: Internet governance and cyber norms
12	11/23/2020	**War Game 1**
13	11/30/2020	**War Game 2**
14	12/06/2020	Reflections: Future of the Internet and conflict studies **Team after-action report due at 11:59 pm on December 15, 2020**

Detailed Course Schedule

Week 1. Introduction, the Internet

- Leiner, Barry Vinton Cerf, David Clark, Robert Kahn, Leonard Kleinrock, Daniel Lynch, Jon Postel, Larry Roberts, and Stephen Wolff. *Brief History of the Internet*, Internet Society, 1997.
- Singer, P.W. and Allan Friedman. *Cybersecurity and Cyberwar.* Oxford University Press (2014): 1-72.
- World Science Festival. 2-13. "A Packet's Tale: How does the Internet work?", URL: https://www.youtube.com/watch?v=ewrBalT_eBM.

Recommended Readings:

- Clark, David D., and Susan Landau. "Untangling Attribution." *Harv. Nat'l Sec. J.* 2 (2011): 323.
- DeNardis, Laura. *The Global War for Internet Governance.* Yale University Press, 2014. Chapters 1-3.
- Rid, Thomas, and Ben Buchanan. "Attributing Cyber Attacks." *Journal of Strategic Studies* 38.1-2 (2015): 4-37.

Week 2. Internet and politics

- Farrell, Henry. "The Consequences of the Internet for Politics." *Annual Review of Political Science* 15 (2012): 35-52.
- Diamond, Larry. "Liberation Technology." *Journal of Democracy* 21.3 (2010):69?83.
- Clinton, Hillary Rodham. "Remarks on Internet Freedom." *US Department of State* 21 (2010).

Recommended Readings:

- Choucri, Nazli, and David D. Clark. *International Relations in the Cyber Age: The co-evolution dilemma.* Information Policy, 2018. Chapter 2.
- Zeitzoff, Thomas. "How Social Media Is Changing Conflict," *Journal of Conflict Resolution* 61.9 (2017): 1970-91.

Week 3. Why control the Internet?

- Wu, Tim, and Jack Goldsmith. *Who Controls the Internet?: Illusions of a borderless world.* Oxford University Press, 2005. Chapter 5.

- Schmidt, E., and Jared Cohen. "The Future of Internet Freedom." *The New York Times. http://www.nytimes.com/2014/03/12/opinion/the-future-of-internet-freedom.html* (2014).
- Tucker, Joshua A., et. al. "From Liberation to Turmoil: Social media and democracy." *Journal of Democracy* 28.4 (2017): 46-59.

Recommended Readings:

- Schneier, Bruce. *Data and Goliath: The hidden battles to collect your data and control your world.* WW Norton & Company, 2015. Chapters TBA.
- DeNardis, Laura. *The Global War for Internet Governance.* Yale University Press, 2014. Chapter TBA
- Gohdes, Anita R. "Repression Technology: Internet accessibility and state violence," *American Journal of Political Science*, forthcoming.

Week 4. Concepts and theories of cyberattacks

- Gartzke, Erik. "The Myth of Cyberwar: Bringing war in cyberspace back down to earth." *International Security* 38.2 (2013): 41-73.
- Rid, Thomas. "Cyber War Will Not Take Place." *Journal of Strategic Studies* 35.1 (2012): 5-32.
- F-Secure Podcast: Episode 20 — Defining Cyber Warfare, with Mikko Hypponen. URL: https://blog.f-secure.com/podcast-cyber-warfare-mikko/.
- Singer, Peter, and August Cole. "The Reality of Cyberwar," *Politico*, 2015.

Recommended Readings:

- Nye, Joseph S. *The Future of Power.* Public Affairs (2011): 126-45.
- Sanger, David E. *The Perfect Weapon: War, sabotage, and fear in the cyber age.* Broadway Books, 2019.
- Buchanan, Ben. *The Cybersecurity Dilemma: Hacking, trust, and fear between nations.* Oxford University Press, 2016.
- Slayton, Rebecca. "What is the Cyber Offense-Defense Balance? Conceptions, causes, and assessment." *International Security* 41.3 (2017): 72-109.

Week 5. Conflict prevention: censorship and net restrictions (domestic)

- Roberts, Sarah T. "Social Media's Silent Filter." *The Atlantic* 8 (2017).
- Myers West, Sarah. "Censored, Suspended, Shadowbanned: User interpretations of content moderation on social media platforms." *New Media & Society* 20.11 (2018): 4366-4383.
- Zittrain, Jonathan and John Palfrey. "Internet Filtering: The politics and mechanisms of control," Deibert, Ronald, John Palfrey, Rafal Rohozinski, Jonathan Zittrain, and Janice Gross Stein (eds) *Access Denied: The practice and policy of global internet filtering.* Cambridge, MA: MIT Press, 2008. Chapters 1, 3.

Recommended Readings:

- King, Gary, Jennifer Pan, and Margaret E. Roberts. "How Censorship in China Allows Government Criticism but Silences Collective Expression," *American Political Science Review* 107.2 (2013): 326-43.
- Mou, Yi, Kevin Wu, and David Atkin. "Understanding the Use of Circumvention Tools to Bypass Online Censorship," *New Media & Society* 18.5 (2016): 837-56.
- Gillespie, Tarleton. *Custodians of the Internet: Platforms, content moderation, and the hidden decisions that shape social media.* Yale University Press, 2018.
- Roberts, Margaret E. *Censored: Distraction and diversion inside China's Great Firewall.* Princeton University Press, 2018.

Week 6. Conflict prevention: deterrence (foreign)

- Libicki, Martin C. *Crisis and Escalation in Cyberspace.* Rand Corporation, 2012: 99-114.
- Lukasik, Stephen J. "A Framework for Thinking about Cyber Conflict and Cyber Deterrence with Possible Declaratory Policies for these Domains." *Proceedings of a Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for US Policy* 2 (2010): 99-121.
- Zetter, Kim. *Countdown to Zero Day: Stuxnet and the launch of the world's first digital weapon.* Broadway books, 2014. Chapter 4.

Recommended Readings:

- Cunningham, Fiona S. "Maximizing Leverage: Explaining China's cyber force posture." *Working Paper.*
- Kostyuk. Nadiya. "Cyber Institutions and Sub-optimal Logic of Cyber Deterrence." *Working Paper.*
- Lindsay, Jon R. "Tipping the Scales: The attribution problem and the feasibility of deterrence against cyberattack." *Journal of Cybersecurity* 1.1 (2015): 53-67.

Week 7. Conflict onset (domestic)

- Weidmann, Nils B., and Espen Geelmuyden Rød. *The Internet and Political Protest in Autocracies.* Oxford Studies in Digital Politics, 2019. Chapter 2.
- Howard, Philip N., and Muzammil M. Hussain. *Democracy's Fourth Wave?: Digital media and the Arab Spring.* Oxford University Press, 2013. Chapters TBA.
- Warren, T. Camber. "Explosive Connections?: Mass media, social media, and the geography of collective violence in African states." *Journal of Peace Research* 52.3 (2015): 297-311.

Recommended Readings:

- Youmans, William Lafi, and Jillian C. York. "Social Media and the Activist Toolkit: User agreements, corporate interests, and the information infrastructure of modern social movements." *Journal of Communication* 62.2 (2012): 315-329.
- Valenzuela, Sebastián. "Unpacking the Use of Social Media for Protest Behavior: The roles of information, opinion expression, and activism," *American Behavioral Scientist* 57.7 (2013): 920?42.
- Steinert-Threlkeld, Zachary C. "Spontaneous Collective Action: Peripheral mobilization during the Arab Spring." *American Political Science Review* 111.2 (2017): 379?403.
- Little, Andrew T. "Communication Technology and Protest," *The Journal of Politics* 78.1 (2015): 152-66.

Week 8. Conflict onset (foreign)

- Axelrod, Robert and Rumen Iliev. "The Timing of Cyber Conflict," *Proceedings of the National Academy of Sciences* 111.4 (2014): 1298-1303.
- Lin, Herbert. "Escalation Dynamics and Conflict Termination in Cyberspace." *Strategic Studies Quarterly* 6.3 (2012): 46-70.
- Healey, Jason. "The Cartwright Conjecture: The deterrent value and escalatory risk of fearsome cyber capabilities." *Working Draft, Available at SSRN 2836206* (2016).

Recommended Readings:

- Herr, Trey, and Drew Herrick. "Military Cyber Operations: A primer." *American Foreign Policy Council Defense Technology Program Brief* 14 (2016).
- Smeets, Max. "The Strategic Promise of Offensive Cyber Operations." *Strategic Studies Quarterly* 12.3 (2018): 90-113.
- Gomez, Miguel Alberto N. "Arming Cyberspace: The militarization of a virtual domain." *Global Security and Intelligence Studies* 1.2 (2016): 5.

Week 9. Conflict intensity and duration (domestic)

- Zeitzoff, Thomas. "Does Social Media Influence Conflict?: Evidence from the 2012 Gaza conflict," *Journal of Conflict Resolution* 62.1 (2018): 29-63.
- Duvanova, Dinissa et al. "Violent Conflict and Online Segregation: An analysis of social network communication across Ukraine's regions." *Journal of Comparative Economics* 44.1 (2016): 163-81.
- Gohdes, Anita R. "Pulling the Plug: Network disruptions and violence in civil conflict," *Journal of Peace Research* 52.3 (2015): 352-67.

Recommended Readings:

- Howard, Philip N., and Muzammil M. Hussain. *Democracy's Fourth Wave?: Digital media and the Arab Spring.* Oxford University Press, 2013. Chapters TBA.
- Weidmann, Nils B., and Espen Geelmuyden Rød. *The Internet and Political Protest in Autocracies.* Oxford Studies in Digital Politics, 2019. Chapters TBA.
- Barberá, Pablo, et.al. "The Critical Periphery in the Growth of Social Protests." *PLOS ONE* 10.11 (2015): e0143611.

Week 10. Conflict intensity and duration (foreign)

- Ottis, Rain. "Analysis of the 2007 Cyber Attacks against Estonia from the Information Warfare Perspective." *Proceedings of the 7th European Conference on Information Warfare.* 2008.
- Perlroth, Nicole, Mark Scott, and Sheera Frenkel. "Cyberattack Hits Ukraine then Spreads Internationally." *The New York Times 27* (2017): 2017.
- Kostyuk, Nadiya and Yuri M. Zhukov. 2019 "Invisible Digital Front: Can cyber attacks shape battlefield events?" *Journal of Conflict Resolution* 63 (2): 317-347
- Grohe, Edwin. "The Cyber Dimensions of the Syrian Civil War: Implications for future conflict." *Comparative Strategy* 34.2 (2015): 133-148.

Recommended Readings:

- The New York Times Daily Podcast, June 18 2019: Hacking the Russian Power Grid: https://www.nytimes.com/2019/06/18/podcasts/the-daily/trump-russia-cyber-grid.html
- Zetter, Kim. "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid." *Wired* (2016).
- Movie: Zero Days (a movie about Stuxnet): http://www.zerodaysfilm.com/

Week 11. Future of the Internet: Internet governance and cyber norms

- Mueller, M. L. "China and global Internet governance: A tiger by the tail." *Access contested: Security, identity, and resistance in Asian cyberspace* (2011): 177-194.
- DeNardis, Laura. *The Global War for Internet Governance.* Yale University Press (2014). Chapter TBA
- Kerr, Jaclyn A. "Rewiring Authoritarianism: The evolution of Internet policy in Putin's Russia." *Working Paper* (2016).

Recommended Readings:

- Shen, Hong. "China and Global Internet Governance: Toward an alternative analytical framework." *Chinese Journal of Communication* 9.3 (2016): 304-324.
- Flyverbom, Mikkel, Ronald Deibert, and Dirk Matten. "The Governance of Digital Technology, Big Data, and the Internet: New roles and responsibilities for business." *Business & Society* 58.1 (2019): 3-19.
- Finnemore, Martha, and Duncan B. Hollis. "Constructing Norms for Global Cybersecurity." *American Journal of International Law* 110.3 (2016): 425-479.
- Deibert, Ronald J. "Toward a Human-Centric Approach to Cybersecurity." *Ethics & International Affairs* 32.4 (2018): 411-424.
- Singer, P.W. and Allan Friedman. *Cybersecurity and Cyberwar.* Oxford University Press (2014): 247-56.

Week 12. War Game Exercise 1

Week 13. War Game Exercise 2

Week 14. Reflections: Internet and conflict studies

- Unver, H. Akin. "Internet, Social Media and Conflict Studies: Can greater interdisciplinarity solve the analytical deadlocks in cybersecurity research?." *arXiv preprint arXiv:1905.01777* (2019).
- Gohdes, Anita R. "Studying the Internet and Violent Conflict," *Conflict Management and Peace Science* 35.1 (2018), 89-106.