GW Elliott School of International Affairs

Fall 2023

IAFF 6186.30

Cyberspace, Conflict, and War

Syllabus

Instructor: Nicholas Anderson

Course Details

Modality: In-Person

Course Description & Goals

This MA seminar course examines the relationship between cyber technology, conflict, and war. After introducing key concepts, capabilities, and actors in cyberspace, the course will examine the relationship between information technology and various aspects of domestic and international conflict and war. These include cyberwar, deterrence and compellence, offense and defense, cyber conflict and escalation, espionage, conventional military operations, nuclear weapons, political subversion, mobilization and repression, civil war, and the laws of armed conflict, among others. These various aspects of cyberspace and conflict will be highlighted through in-depth examinations of key academic and policy debates as well as crucial contemporary case studies. Through this course, students will gain a thorough understanding of how cyber technology is shaping domestic and international conflict.

Learning Outcomes & Objectives

By the end of this course, students will be able to:

- Demonstrate a deep understanding of the basic structure of cyberspace and key cyber technologies.
- Identify the primary actors, their cyber capabilities, and their varied approaches to cyberspace.
- Critically engage cutting-edge academic research on cyberspace and conflict.
- Critically engage the most important policy debates on cyberspace and conflict.
- Write for a policy audience.

Methods of Instruction

This course uses the following methods of instruction:

- ***Readings:*** Readings are assigned for each class, including the first and final sessions. There are also optional "suggested readings," for those who would like to delve deeper into given topics.

- ***Lectures:*** While this is a discussion-based seminar course, the sessions will be interspersed with lecture material from the professor.
- ***Discussion:*** Student-led discussion will comprise the majority of class time each week.
- ***Writing assignments:*** There are three written assignments—two policy memos and a final policy paper.

Credit Hour Policy

In this 3-credit graduate course, students are expected to work for approximately 450 minutes per week. This includes about 100 minutes of lecture and discussion time in class, and about 350 minutes (nearly 6 hours) on reading, note taking, writing assignments, and review. In total, you are expected to work for at least 112.5 hours over the duration of this 15-week semester.

Prerequisites

Academic

There are no academic prerequisites for this course. Note that a background in information technology or computer science is ***not*** assumed.

Technological

As a graduate student, it is necessary to possess baseline technology skills in order to participate fully in the course. Please consult the GW Online website for further information about recommended configurations and support. If you have questions or problems with technology for this course, please consult the Technology Help link in the left navigation menu in our course in Blackboard.

You should be able to:

- Use a personal computer and its peripherals.
- Use word processing and other productivity software.
- Access course materials on Blackboard and the GW Library website.
- Use the webcam and microphone on your device (for periodic virtual office hours).
- Seek technology help by contacting GW Information Technology (202-994-4948).

Course Materials & Requirements

There are no required texts or other materials for the course, though (almost) all of the book excerpts assigned in this course are from books that I would recommend purchasing if you are interested.

Feedback

I would appreciate your feedback throughout the semester on how the course is going. Please feel free to email me, come to my office hours, or provide anonymous feedback at the following link:

Grading & Assessment

This course uses a percent-based grading schema, as shown below.

Assignment Type	*Length*	*Due date*	*Total % of Final Grade*
Attendance and Participation			20%
Policy Memo #1	500 words	Session 5 (2 Oct.)	20%
Policy Memo #2	500 words	Session 9 (30 Oct.)	20%
Policy Paper	2,000 words	18 Dec.	40%
			Total Percent: 100%

The grading scale below, determines your final letter grade.

Excellent	**Good**	**Needs Improvement**	**Low Pass**	**Fail**
A 94%-100%	B+ 87%-89%	B- 80%-83%	C 74%-76%	F Under 70%
A- 90%-93%	B 84%-86%	C+ 77%-79%	C- 70%-73%	

ASSIGNMENTS

- **Attendance and Participation (20%):** This is a seminar, not a lecture course. Student participation is essential. Students are expected to attend all sessions, arrive on time, have read all of the items listed under "Required Readings" prior to each session, and be prepared to discuss the issues under consideration for that session. If—for any reason—active, verbal, and regular participation is a problem for you, please contact the instructor directly and we can work out alternatives.

- **Policy Memo #1 (20%), Due Session 5 (2 Oct.) @ 7:10 PM:** Write a short, persuasive policy memo responding to, and taking a position on, a key question of policy concern regarding cyberspace and conflict. Students will choose from the following questions:

    1. Should cyberspace be considered a distinct "domain" of war, like land, sea, air, and outer space? Why or why not?
    2. What are three key characteristics of cyber "weapons"? How do they influence how they can be used?
    3. Has the emergence of cyber technology led to an important shift in the balance of power? Why or why not?
    4. Should the United States (or any other country of your choice) legalize offensive cyber operations by private actors? Why or why not?

    Your paper should (i) directly respond to the prompt; (ii) take a clear position on the policy question; (iii) support your position with logical argumentation and/or evidence; and (iv) discuss the policy implications of your chosen position. The best answers will do all of this while incorporating ideas from multiple sessions. Your paper should be presented in a professional manner, written in clear and concise prose, and be free of typos and other errors.

The paper should be double spaced and ***no more*** than 500 words in length. Use standard (12-point) font and standard (1-inch) margins. No references or citations are necessary. Please submit your paper anonymized (GWID Number only, filename: "G##########_Memo1") and in Microsoft Word format via Blackboard (under "Assignments").

- **Policy Memo #2 (20%), Due Session 9 (30 Oct.) @ 7:10 PM:** Write a short, persuasive policy memo responding to, and taking a position on, a key question of policy concern regarding cyberspace and conflict. Students will choose from the following questions:

    1. Is deterrence a credible strategy in cyberspace? Why or why not?
    2. Should U.S. Cyber Command continue to pursue a policy of "persistent engagement"? Why or why not?
    3. Is the cyber domain offense-dominant when it comes to cyber conflict? Why or why not?
    4. Is escalation in cyber conflict a serious concern? Why or why not?

  Your paper should (i) directly respond to the prompt; (ii) take a clear position on the policy question; (iii) support your position with logical argumentation and/or evidence; and (iv) discuss the policy implications of your chosen position. The best answers will do all of this while incorporating ideas from multiple sessions. Your paper should be presented in a professional manner, written in clear and concise prose, and be free of typos and other errors.

  The paper should be double spaced and ***no more*** than 500 words in length. Use standard (12-point) font and standard (1-inch) margins. No references or citations are necessary. Please submit your paper anonymized (GWID Number only, filename: "G##########_Memo2") and in Microsoft Word format via Blackboard.

- **Policy Paper (40%), Due 18 December @ 11:59:59 PM:** Write a policy paper that analyzes a key question of policy concern regarding cyberspace and conflict. Students will choose from the following questions and topics:

    1. Student choice: Research and write a paper on a topic of your choice related to cybersecurity and conflict that has clear policy relevance. It ***must*** be cleared in advance by the instructor.
    2. Has the emergence and spread of cyber technology revolutionized international security? Why or why not?
    3. Conduct an assessment of the cyber power of a state of your choosing. How does it rank in terms of global cyber power? What does this suggest about the relationship between cyber power and national power?
    4. Is cyber terrorism or terrorist use of cyberspace a significant national security concern? Why or why not? Is this likely to change?
    5. Is cyberwar "war" or is it something else, like espionage, sabotage, and/or subversion?
    6. Conduct an assessment of a conventional military operation of your choosing that included an important cyberspace component, such as Georgia (2008), Gaza (2012), Ukraine I (2014-), or Ukraine II (2022-). What role did cyber capabilities play in this conflict? What difference did they make? What does your answer suggest about the present and future relationship between conventional war and cyberspace?
    7. Are information technologies more "liberation technologies" or "repression technologies"? Why?

8. How do the Laws of Armed Conflict apply to cyberspace? What are some of the challenges associated with their application? What are some solutions?

Your paper should (i) directly respond to the prompt; (ii) take a clear position on the policy question; (iii) support your position with logical argumentation and evidence; (iv) discuss the policy implications of your chosen position; and (v) most importantly, draw on a wide variety of course materials. Your paper should be presented in a professional manner, written in clear and concise prose, and be free of typos and other errors.

The paper must be double spaced and ***no more* than 2,000 words** in length (**not** including citations). Use standard (12-point) font and standard (1-inch) margins. Chicago-style footnotes for citations and references is preferred. Please do not use endnotes. No bibliography is necessary. Please reference the Chicago Manual of Style Citation Quick Guide if needed. Please submit your paper anonymized (GWID Number only, filename: "G##########_Final") and in Microsoft Word format via Blackboard.

Course Calendar & Readings

Session 1 (28 Aug.): Introduction, the Cyber Revolution, & a Brief History of Cyberspace

Key Concepts & Discussion Questions:

- Key Concepts: cyberspace; cybersecurity; communication link; router, packet; cryptography; Internet Protocol (IP); Internet Service Provider (ISP); Hypertext Transfer Protocol (HTTP) system; Uniform Resource Locator (URL); Domain Name System (DNS); Internet of Things.
- Has information technology revolutionized international relations? If so, how? If not, why not?
- What are some of the specific national and international security challenges brought about by the rise of information technology? Which are ameliorated?

Required Readings (~105 pages):

- William J. Lynn III, "Defending a New Domain: The Pentagon's Cyberstrategy," *Foreign Affairs*, Vol. 89, No. 5 (September/October 2010), pp. 97-108 (GWU library link).
- Lucas Kello, "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft," *International Security*, Vol. 38, No. 2 (Fall 2013), pp. 7-40 (GWU library link).
- P. W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (New York: Oxford, 2014), pp. 1-34 (GWU library link).
- David Clark, Thomas Berson, and Herbert S. Lin, eds., *At the Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues* (Washington: The National Academies Press, 2014), pp. 7-28 (GWU library link).
- **Watch:** "How the Internet Works," Khan Academy & Code.org (2021) (7 videos, from "What is the Internet?" to "Cybersecurity and Crime") (External link).
- ***Skim:*** "Good Cyber Hygiene Habits to Help Stay Safe Online," Norton (23 January 2021) (External link).

Recommended Readings:

- David D. Clark, "An Insider's Guide to the Internet," *Unpublished Manuscript, MIT* (2004).
- Barry M. Leiner, et al., "A Brief History of the Internet," *ACM SIGCOMM Computer Communication Review*, Vol. 39, No. 5 (October 2009), pp. 22-31.

- Alexander Klimburg, *The Darkening Web: The War for Cyberspace* (New York: Penguin, 2017), pp. 23-51.

Reminder (4 Sept.): No Class (Labor Day)

Session 2 (11 Sept.): Key Concepts & Capabilities in Cyberspace

Key Concepts & Discussion Questions:

- Key Concepts: cyberattack; cyber exploitation; vulnerability; bug; back door; zero-day vulnerability; remote access; close access; social access; payload; malware; worm; denial-of-service (DoS) attack; distributed denial-of-service (DDoS) attack; botnet; phishing; spear phishing; hacker; advanced persistent threat (APT); air gap; firewall; patching; critical infrastructure; supervisory control and data acquisition (SCADA) systems.
- Should cyberspace be considered a distinct "domain" of war, like land, sea, air, and outer space?
- In 2018, the U.S. Department of Defense established Cyber Command (CYBERCOM) as one of its eleven combatant commands. Should cyberspace have its own command? Why or why not?
- What are some of the key characteristics of cyber weapons that make them distinct from conventional weapons?
- Where should we draw the line between what counts as a cyber weapon and what doesn't?
- Are cyber weapons "weapons"? If so, in what ways? If not, why not?

Required Readings (~82 pages):

- P. W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (New York: Oxford, 2014), pp. 34-72 (GWU library link).
- David Clark, Thomas Berson, and Herbert S. Lin, eds., *At the Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues* (Washington: The National Academies Press, 2014), pp. 29-52 (GWU library link).
- Thomas Rid and Peter McBurney, "Cyber-Weapons," *The RUSI Journal*, Vol. 157, No. 1 (February/March 2012), pp. 6-13 (GWU library link).
- Robert Axelrod and Rumen Iliev, "Timing of Cyber Conflict" *Proceedings of the National Academy of Sciences*, Vol. 111, No. 4 (28 January 2014), pp. 1298-1303 (GWU library link).
- ***Skim:*** "The 14 Most Common Cyber Attacks," Crowdstrike (30 September 2021) (External link).

Recommended Readings:

- Herbert Lin, "A Virtual Necessity: Some Modest Steps Toward Greater Cybersecurity," *Bulletin of the Atomic Scientists*, Vol. 68, No. 5 (2012), 75-87.
- Peter Dombrowski and Chris C. Demchak, "Cyber War, Cybered Conflict, and the Maritime Domain," *Naval War College Review*, Vol. 67, No. 2 (Spring 2014), pp. 71-96 (esp. 73-76).
- Martin C. Libicki, *Cyberspace in Peace and War* (Annapolis: Naval Institute Press, 2016), Chs. 2, 4.
- Alexander Klimburg, *The Darkening Web: The War for Cyberspace* (New York: Penguin, 2017), pp. 53-65.

- Ioannis Agrafiotis et al., "A Taxonomy of Cyber Harms: Defining the Impacts of Cyber-Attacks and Understanding How They Propagate," *Journal of Cybersecurity*, Vol. 4, No. 1 (2018), pp. 1-15.
- Nazli Choucri and David D. Clark, *International Relations in the Cyber Age: The Co-Evolution Dilemma* (Cambridge: MIT Press, 2018), pp. 33-66 (Ch. 2).
- Max Smeets, "A Matter of Time: On the Transitory Nature of Cyber Weapons," *Journal of Strategic Studies*, Vol. 41, No. 1-2 (2018), pp. 6-32.
- Jacquelyn Schneider, "The Capability/Vulnerability Paradox and Military Revolutions: Implications for Computing, Cyber, and the Onset of War," *Journal of Strategic Studies*, Vol. 42, No. 6 (2019), pp. 841-863.
- Brendan Rittenhouse Green and Austin Long, "Conceal or Reveal? Managing Clandestine Military Capabilities in Peacetime Competition," *International Security*, Vol. 44, No. 3 (Winter 2019/2020), pp. 48-83.
- Rebecca Slayton, "What is a Cyber Warrior? The Emergence of U.S. Military Cyber Expertise, 1967–2018," *Texas National Security Review*, Vol. 4, No. 1 (Winter 2020/2021), pp. 71-96.
- Jordan Branch, "What's in a Name? Metaphors and Cybersecurity," *International Organization*, Vol. 75, No. 1 (Winter 2021), pp. 39-70.
- Max Smeets, "Cyber Arms Transfer: Meaning, Limits, and Implications," *Security Studies*, Vol. 31, No. 1 (2022), pp. 65-91.

Session 3 (18 Sept.): Cyberpower & the Great Powers

Key Concepts & Discussion Questions:

- Key Concepts: power; cyber power; diffusion; the "three faces" of power; Operation Olympic Games; Stuxnet.
- Is power a property or a relation? Is it about the "stuff" you have or the influence gives you?
- What are some of the key attributes of the states with the strongest cyber capabilities?
- What are some of the ways of measuring cyber power? Which are more/less useful?
- What are the costs and benefits of a quantitative vs. a qualitative approach to measuring cyber power?
- Why is measuring cyber power hard?
- Why are cyber capabilities often referred to as "weapons of the weak"? Do you agree with this characterization?

Required Readings (146 pages):

- Joseph S. Nye, Jr., *The Future of Power: Its Changing Nature and Use in the Twenty-First Century* (New York: PublicAffairs, 2011), pp. 113-151(Ch. 5) (GWU library link).
- Adam Segal, *Hacked World Order: How States Fight, Trade, Maneuver, and Manipulate in the Digital Age* (New York: Public Affairs, 2016), pp. 27-49 (Ch. 2) (On Blackboard).
- *Cyber Capabilities and National Power: A Net Assessment* (London: The International Institute for Strategic Studies, 2021), pp. 1-13, 15-27 (U.S.), 89-114 (China, Russia), 171-174 (External link).
- ***Skim:*** Julia Voo, Ifran Hemani, and Daniel Cassidy, *National Cyber Power Index 2022: Methodology and Analytical Considerations* (Cambridge: Belfer Center for Science and International Affairs, September 2022), pp. 2-3, 9-14, 17-21 (External link).

- Nicole Perlroth, *This is How They Tell Me the World Ends* (New York: Bloomsbury, 2021), pp. 117-131 (Ch. 9) (On Blackboard).

Recommended Readings:

- Jon R. Lindsay, "The Impact of China on Cybersecurity: Fiction or Friction?" *International Security*, Vol. 39, No. 3 (Winter 2014/2015), pp. 7-47.
- Brandon Valeriano and Ryan C. Maness, *Cyber War vs. Cyber Realities: Cyber Conflict in the International System* (New York: Oxford University Press, 2015), pp. 24-28.
- *Zer0 Days*, Directed by Alex Gibney, Magnolia Pictures, 2016.
- Alexander Klimburg, *The Darkening Web: The War for Cyberspace* (New York: Penguin, 2017), pp. 301-314.
- Tarun Chaudhary, Jenna Jordan, Michael Salomone, and Phil Baxter, "Patchwork of Confusion: The Cybersecurity Coordination Problem," *Journal of Cybersecurity*, Vol. 4, No. 1 (2018), pp. 1-13.
- Brandon Valeriano, Benjamin Jensen, and Ryan C. Maness, *Cyber Strategy: The Evolving Character of Power and Coercion* (New York: Oxford University Press, 2018), pp. 59-61, 72-74.
- "Ch. 10: Military Cyber Capabilities," in *The Military Balance*, Vol. 120 (London: International Institute of Strategic Studies, 2020), pp. 515-518.
- Julia Voo, Ifran Hemani, Simon Jones, Winnona DeSombre, Dan Cassidy, and Anina Schwarzenbach, *National Cyber Power Index 2020: Methodology and Analytical Considerations* (Cambridge: Belfer Center for Science and International Affairs, September 2020), pp. 4-6, 11-15, 20-25, 26-45 (External link).
- "Ch. 10: Military Cyber Capabilities," in *The Military Balance*, Vol. 122 (London: International Institute of Strategic Studies, 2022), pp. 507-510.
- Fiona S. Cunningham, "Strategic Substitution: China's Search for Coercive Leverage in the Information Age," *International Security*, Vol. 47, No. 1 (Summer 2022), pp. 46-92.
- Erica D. Lonergan and Jacquelyn Schneider, "The Power of Beliefs in US Cyber Strategy: The Evolving Role of Deterrence, Norms, and Escalation," *Journal of Cybersecurity*, Vol. 9, No. 1 (2023), pp. 1-10.

Session 4 (25 Sept.): Minor Powers & Non-State Actors in Cyberspace

Key Concepts & Discussion Questions:

- Key Concepts: non-state actor; terrorism; transnational terrorism; domestic terrorism; cyber terrorism; cyber proxy; patriotic hacker; hacktivist; cyber criminal; cybersecurity contractor; NSO Group; Pegasus.
- Who are some of the key non-state actors that are active in cyberspace?
- Why do so many see cyberspace empowering non-state actors?
- Why do so many see cyber terrorism as a key threat of the information age?
- Why does Benson argue that the internet does not empower terrorists? Do you agree?
- What are the basic forms of control over proxies according to Maurer? How does this relate to domestic politics?
- What are some of the positive and negative consequences of empowering the private sector to engage in offensive cyber operations, according to Kello? Do you agree?
- Is the U.S. at a disadvantage vis-à-vis China (patriotic hackers) and/or Russia (cyber criminals) when it comes to the use of cyber proxies?

Required Readings (~125 pages):

- *Cyber Capabilities and National Power: A Net Assessment* (London: The International Institute for Strategic Studies, 2021), pp. 69-78 (Israel), 115-132 (Iran, North Korea) (External link).
- David C. Benson, "Why the Internet is Not Increasing Terrorism," *Security Studies*, Vol. 23, No. 2 (2014), pp. 293-328 (GWU library link).
- Tim Maurer, "Cyber Proxies and Their Implications for Liberal Democracies," *The Washington Quarterly*, Vol. 41, No. 2 (Summer 2018), pp. 171-188 (GWU library link).
- Lucas Kello, "Ch. 15: Private Sector Cyber Weapons: An Adequate Response to the Sovereignty Gap?" in Herbert Lin and Amy Zegart, eds., *Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations* (Washington: Brookings Institution Press, 2019), pp. 357-378 (GWU library link).
- Dana Priest, et al., "Private Israeli Spyware Used to Hack Cellphones of Journalists, Activists Worldwide," *The Washington Post* (18 July 2021) (External link).

Recommended Readings:

- Alexander Klimburg, "Mobilising Cyber Power," *Survival*, Vol. 53, No. 1 (February-March 2011), pp. 41-60.
- Brandon Valeriano and Ryan C. Maness, *Cyber War vs. Cyber Realities: Cyber Conflict in the International System* (New York: Oxford University Press, 2015), Ch. 7.
- Tim Maurer, *Cyber Mercenaries: The State, Hackers, and Power* (New York: Cambridge University Press, 2017).
- William Akoto, "Accountability and Cyber Conflict: Examining Institutional Constraints on the use of Cyber Proxies," *Conflict Management and Peace Science*, Vol. 39, No. 3 (2022), pp. 311-332.
- Ryan Shandler, Michael L. Gross, Sophia Backhaus, and Daphna Canetti, "Cyber Terrorism and Public Support for Retaliation – A Multi-Country Survey Experiment," *British Journal of Political Science*, Vol. 52, No. 2 (2022), pp. 850-868.
- *Global Spyware Scandal: Exposing Pegasus*, Directed by Anne Poiret and Arthur Bouvart, PBS Frontline (2023) (External link).
- Justin Key Canfil, "The illogic of plausible deniability: why proxy conflict in cyberspace may no longer pay," *Journal of Cybersecurity*, Vol. 8, No. 1 (2022), pp. 1-16.

Session 5 (2 Oct.): Cyberwar & Cyber Conflict (*Policy Memo #1 Due*)

Key Concepts & Discussion Questions:

- Key Concepts: war; cyberwar; subversion; espionage; sabotage; intelligence contest.
- What is cyberwar?
- Why does Rid argue that cyberwar will not take place? Is he right?
- Why does Gartzke argue that cyberwar is largely a myth? Is he right?
- Do you agree with Rovner's characterization of cyber conflict as an "intelligence contest"?
- What do the data collected and presented by Maness and coauthors reveal about cyber conflict?
- Why are the most catastrophic attacks in cyberspace so rare, or even non-existent?

- What are some of the benefits of referring to conflict in cyberspace as war? What are some of the risks?

Required Readings (~106 pages):

- Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to do About It* (New York: Ecco, 2010), pp. 64-68 (On Blackboard).
- Thomas Rid, "Cyber War Will Not Take Place," *Journal of Strategic Studies*, Vol. 35, No. 1 (February 2012), pp. 5-32 (GWU library link).
- Erik Gartzke, "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth," *International Security*, Vol. 38, No. 2 (Fall 2013), pp. 41-73 (GWU library link).
- Joshua Rovner, "Cyberwar as an Intelligence Contest" *War on the Rocks* (16 September 2019) (External link).
- Farnaz Fassihi and Ronen Bergman, "Israel and Iran Broaden Cyberwar to Attack Civilian Targets," *The New York Times* (27 November 2021) (External link).
- Ryan C. Manness, Brandon Valeriano, Benjamin Jensen, Kathryn Hedgecock, and Jose Macias, "Expanding the Dyadic Cyber Incident and Dispute (DCID) Dataset: Cyber Conflict," *Cyber Defense Review*, forthcoming (2023), pp. 2-3, ***skim*** 3-13, 13-27 (On Blackboard).

Recommended Readings:

- John Arquilla and David Ronfeldt, "Chapter 2: Cyberwar is Coming!" in John Arquilla and David Ronfeldt, eds., *In Athena's Camp: Preparing for Conflict in the Information Age* (Santa Monica: RAND Corporation, 1997), pp. 23-32.
- Adam P. Liff, "Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War," *Journal of Strategic Studies*, Vol. 35, No. 3 (June 2012), pp. 401-428.
- Jon R. Lindsay, "Stuxnet and the Limits of Cyber Warfare," *Security Studies*, Vol. 22, No. 3 (2013), pp. 365-404.
- Brandon Valeriano and Ryan C. Manness, "The Dynamics of Cyber Conflict Between Rival Antagonists, 2001-11," *Journal of Peace Research*, Vol. 51, No. 3 (2014), pp. 347-360.
- Peter W. Singer and August Cole, "The Reality of Cyberwar," *Politico Magazine* (9 July 2015).
- Ryan C. Maness and Brandon Valeriano, "The Impact of Cyber Conflict on International Interactions," *Armed Forces & Society*, Vol. 42, No. 2 (2016), pp. 301-323.
- Brandon Valeriano, Benjamin Jensen, and Ryan C. Maness, *Cyber Strategy: The Evolving Character of Power and Coercion* (New York: Oxford University Press, 2018), pp. 66-68.
- Travis Sharp, "Hiding in Plain Sight: Political Effects of Cyber Operations," *Survival*, Vol. 60, No. 6 (2018), pp. 45-53.
- William Ralston, "The Untold Story of a Cyberattack, a Hospital and a Dying Woman," *Wired* (11 November 2020) (External link).
- Lennart Maschmeyer, "The Subversive Trilemma: Why Cyber Operations Fall Short of Expectations," *International Security*, Vol. 46, No. 2 (2021), pp. 51-90.
- Kevin Poulson, Robert McMillan, and Melanie Evans, "A Hospital Hit by Hackers, a Baby in Distress: The Case of the First Alleged Ransomware Death," *The Wall Street Journal* (30 Sept. 2021) (External link).

- William Akoto, "International Trade and Cyber Conflict: Decomposing the Effects of Trade on State-Sponsored Cyber Attacks," *Journal of Peace Research*, Vol. 58, No. 5 (2021), pp. 1083-1097.
- Richard J. Harknett and Max Smeets, "Cyber Campaigns and Strategic Outcomes," *Journal of Strategic Studies*, Vol. 45, No. 4 (2022), pp. 534-567.
- Lennart Maschmeyer, "A New and Better Quiet Option? Strategies of Subversion and Cyber Conflict," *Journal of Strategic Studies*, Latest Articles (2022), pp. 1-25.
- Lindsey Guenther and Paul Musgrave, "New Questions for an Old Alliance: NATO in Cyberspace and American Public Opinion," *Journal of Global Security Studies*, Vol. 7, No. 4 (2022), pp. 1-23.
- Lennart Maschmeyer and Myriam Dunn Cavelty, "Goodbye Cyberwar: Ukraine as a Reality Check," *Policy Perspectives*, Vol. 10, No. 3 (May 2022), pp. 1-4 (External link).
- Matthias Schulze, "Quantifying Cyber Conflict: Introducing the European Repository on Cyber Incidents," Lawfare (7 November 2022) (Article external link, Data external link).

Session 6 (9 Oct.): Deterrence & Compellence in Cyberspace

Key Concepts & Discussion Questions:

- Key Concepts: coercion; deterrence; compellence; defense; deterrence by punishment; deterrence by denial; cyber deterrence; resilience; cross-domain deterrence; the attribution problem; cyber persistence; persistent engagement.
- What is required for deterrence to operate?
- Why is it commonly argued that deterrence is difficult or impossible in cyberspace? Do you agree?
- What kind of deterrence might be effective in cyberspace, and why?
- What are some of the important factors that go into the process of attribution, according to Rid and Buchanan?
- If deterrence operates in cyberspace, why do we observe so many attacks? If it doesn't, why do we see so few major attacks?
- How has U.S. strategy in cyberspace changed over the past generation?
- What are some of the benefits associated with persistent engagement? Some of the risks?

Required Reading (~121 pages):

- Jacquelyn G. Schneider, "Deterrence in and Through Cyberspace," in Jon R. Lindsay and Erik Gartzke, eds., *Cross-Domain Deterrence: Strategy in an Era of Complexity* (New York: Oxford University Press, 2019), pp. 95-120 (On Blackboard).
- Michael P. Fischerkeller and Richard J. Harknett, "Deterrence is not a Credible Strategy for Cyberspace," *Orbis*, Vol. 61, No. 3 (Summer 2017), pp. 381-393 (GWU library link).
- Erica D. Borghard and Shawn W. Lonergan, "Deterrence by Denial in Cyberspace," *Journal of Strategic Studies*, Vol. 46, No. 3 (2023), pp. 534-569 (GWU library link).
- Thomas Rid and Ben Buchanan, "Attributing Cyber Attacks," *Journal of Strategic Studies*, Vol. 38, No. 1-2 (2015), pp. 4-37 (GWU library link).
- Paul M. Nakasone and Michael Sulmeyer, "How to Compete in Cyberspace: Cyber Command's New Approach," *Foreign Affairs* (25 August 2020) (External link or on Blackboard).

Suggested Readings:

- Charles L. Glaser, "Deterrence of Cyber Attacks and U.S. National Security," *The George Washington University Cyber Security Policy and Research Institute Report* (June 2011).
- Thomas Rid, *Cyber War Will Not Take Place* (New York: Oxford University Press, 2013), Ch. 7.
- Dorothy E. Denning, "Rethinking the Cyber Domain and Deterrence," *Joint Forces Quarterly*, Vol. 77, No. 2 (2015), pp. 8-15.
- Jon R. Lindsay, "Tipping the Scales: The Attribution Problem and the Feasibility of Deterrence Against Cyberattack," *Journal of Cybersecurity*, Vol. 1, No. 1 (2015), pp. 53-67.
- Robert Jervis, "Some Thoughts on Deterrence in the Cyber Era," *Journal of Information Warfare*, Vol. 15, No. 2 (2016), pp. 66-73.
- Joseph S. Nye Jr., "Deterrence and Dissuasion in Cyberspace," *International Security*, Vol. 41, No. 3 (Winter 2016/17), pp. 44-71.
- Uri Tor, "'Cumulative Deterrence' as a New Paradigm for Cyber Deterrence," *Journal of Strategic Studies*, Vol. 40, No. 1-2 (2017), pp. 92-117.
- Erica D. Borghard and Shawn W. Lonergan, "The Logic of Coercion in Cyberspace," *Security Studies*, Vol. 26, No. 3 (2017), pp. 452-481.
- *Summary: Department of Defense Cyber Strategy, 2018* (Washington: Department of Defense, 2018).
- Lucas Kello, *The Virtual Weapon and International Order* (New Haven: Yale University Press, 2018), Ch. 7.
- Jon R. Lindsay and Erik Gartzke, "Chapter 9: Coercion through Cyberspace: The Stability-Instability Paradox Revisited," in Kelly M. Greenhill and Peter Krause, eds., *Coercion: The Power to Hurt in International Politics* (New York: Oxford University Press, 2018), only pp. 190-203.
- Michael Poznansky and Evan Perkoski, "Rethinking Secrecy in Cyberspace: The Politics of Voluntary Attribution," *Journal of Global Security Studies*, Vol. 3, No. 4 (2018), pp. 402-416.
- Brandon Valeriano, Benjamin Jensen, and Ryan C. Maness, *Cyber Strategy: The Evolving Character of Power and Coercion* (New York: Oxford University Press, 2018), pp. 58-63, 78-83.
- Jason Healey, "Chapter 8: The Cartwright Conjecture: The Deterrent Value and Escalatory Risk of Fearsome Cyber Capabilities," in Herbert Lin and Amy Zegart, eds., *Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations* (Washington: Brookings Institution Press, 2019), pp. 173-194.
- Jon Lindsay and Erik Gartzke, "Chapter 2: Cybersecurity and Cross-Domain Deterrence," in Damien Van Puyvelde and Aaron Brantly, eds., *US National Cybersecurity: International Politics, Concepts and Organization* (New York: Routledge, 2019).
- Paul M. Nakasone, "A Cyber Force for Persistent Operations," *Joint Forces Quarterly*, Vol. 92, No. 1 (2019), pp. 10-14.
- David Blagden, "Deterring Cyber Coercion: The Exaggerated Problem of Attribution," *Survival*, Vol. 62, No. 1 (February-March 2020), pp. 131-148.
- Joseph M. Brown and Tanisha M. Fazal, "#SorryNotSorry: Why States Neither Confirm nor Deny Responsibility for Cyber Operations," *European Journal of International Security*, Vol. 6, No. 4 (November 2021), pp. 401-417.
- Nadiya Kostyuk, "Deterrence in the Cyber Realm: Public vs. Private Capabilities," *International Studies Quarterly*, Vol. 65, No. 4 (December 2021), pp. 1151-1162.

- Marcelo Leal and Paul Musgrave, "Cheerleading in Cyberspace: How the American Public Judges Attribution Claims for Cyberattacks," *Foreign Policy Analysis*, Vol. 18, No. 2 (April 2022), pp. 1-16.
- Gil Baram, "Public Secrets: The Dynamics of Publicity and Secrecy in Offensive Cyber Operations," *Journal of Global Security Studies*, Vol. 8, No. 3 (2023), pp. 1-11.

Session 7 (16 Oct.): Offense, Defense, & Cyberspace

Key Concepts & Discussion Questions:

- Key Concepts: offense-defense balance; security dilemma; arms race; preemptive vs. preventive attack; deception; dissimulation vs. simulation; stability-instability paradox; Ukraine power grid hack(s).
- What kinds of factors favor offense in military technology? What kinds of factors favor defense?
- What are the strategic implications of offense dominance? Defense dominance?
- Why is cyberspace commonly characterized as an offense-dominant domain? Do you agree?
- Why is defense so costly in cyberspace, according to Kello? Do you agree?
- What are some of the problems of applying offense-defense theory to cyberspace, according to Lieber?
- Why does Slayton argue that technology alone is insufficient to determine the offense-defense balance in cyberspace? What does she think needs to be considered, and why?
- How do Gartzke and Lindsay think the offense-defense balance operates in cyberspace? Do you agree?
- What is the significance of Russia's 2015-2016 hacks of Ukraine's power grid? Do you agree that Ukraine is a "test lab" for Russian cyberwar?

Required Readings (~122 pages):

- Keir Lieber, "The Offense-Defense Balance and Cyber Warfare," in Emily O. Goldman and John Arquilla, eds., *Cyber Analogies* (Monterey: Naval Postgraduate School, 2014), pp. 96-107 (GWU library link).
- Lucas Kello, *The Virtual Weapon and International Order* (New Haven: Yale University Press, 2018), Ch. 2 (On Blackboard).
- Rebecca Slayton, "What Is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment," *International Security*, Vol. 41, No. 3 (Winter 2016/17), pp. 72-109 (GWU library link).
- Erik Gartzke and John R. Lindsay, "Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace," *Security Studies*, Vol. 24, No. 2 (2015), pp. 316-348 (GWU library link).
- Andy Greenberg, "How an Entire Nation Became Russia's Test Lab for Cyberwar," *Wired* (20 June 2017) (External link or on Blackboard).

Recommended Readings:

- Thomas Rid, *Cyber War Will Not Take Place* (New York: Oxford University Press, 2013), pp. 167-170.
- Robert M. Lee, et al., *Analysis of the Cyber Attack on the Ukrainian Power Grid* (Washington: EISAC, March 2016).
- Ben Buchanan, *The Cybersecurity Dilemma: Hacking, Trust, and Fear Between Nations* (New York: Oxford University Press, 2017), pp. 103-114.

Session 8 (23 Oct.): Cyber Conflict & Escalation

Key Concepts & Discussion Questions:

- Key Concepts: escalation; deliberate escalation; inadvertent escalation; accidental escalation; catalytic escalation; crisis (in)stability; signaling; means-based vs. effects-based escalation; firebreaks; vertical escalation; horizontal escalation; escalation dominance; operational preparation of the environment (OPE).
- What are some of the pathways, or mechanisms, though which escalation could occur in cyber conflict?
- What are some of the factors that could influence the potential for escalation in cyber conflict?
- Why do Borghard and Lonergan argue that cyber operations are unlikely to escalate? Do you agree?
- What are some of the strengths of the evidence presented by Valeriano, Jensen, and Maness? The weaknesses?
- What are some of the benefits of the experimental method used by Kreps and Schneider? The drawbacks?
- What are the broader implications, if any, of Israel's deadly 2019 airstrike on a Hamas cyber unit?

Required Readings (~83 pages):

- Herbert Lin, "Escalation Dynamics and Conflict Termination in Cyberspace," *Strategic Studies Quarterly*, Vol. 6, No. 3 (Fall 2012), pp. 46-70 (GWU library link).
- Erica D. Borghard and Shawn W. Lonergan, "Cyber Operations and Imperfect Tools of Escalation," *Strategic Studies Quarterly*, Vol. 13, No. 3 (Fall 2019), pp. 122-145 (GWU library link).
- Brandon Valeriano, Benjamin Jensen, and Ryan C. Maness, *Cyber Strategy: The Evolving Character of Power and Coercion* (New York: Oxford University Press, 2018), pp. 53-58, 63-66, 74-78, 83-88 (On Blackboard).
- Sarah Kreps and Jacqueline Schneider, "Escalation Firebreaks in the Cyber, Conventional, and Nuclear Domains: Moving Beyond Effects-Based Logics," *Journal of Cybersecurity*, Vol. 5, No. 1 (2019), pp. 1-11 (GWU library link).
- Lily Hay Newman, "What Israel's Strike on Hamas Hackers Means for Cyberwar," *Wired* (06 May 2019) (External link or on Blackboard).

Recommended Readings:

- David C. Gompert and Martin Libicki, "Cyber Warfare and Sino-American Crisis Instability," *Survival*, Vol. 56, No. 4 (2014), pp. 7-22.
- Martin C. Libicki, *Cyberspace in Peace and War* (Annapolis: Naval Institute Press, 2016), Ch. 27.
- Ryan C. Maness and Brandon Valeriano, "The Impact of Cyber Conflict on International Interactions," *Armed Forces & Society*, Vol. 42, No. 2 (2016), pp. 301-323.
- Jacqueline Schneider, *The Information Revolution and International Stability: A Multi-Article Exploration of Computing, Cyber, and Incentives for Conflict* (Ph.D. Dissertation, The George Washington University, May 2017), pp. 115-159 (Ch. 3).
- Erica D. Borghard and Jacquelyn Schneider, "Israel Responded to a Hamas Cyberattack with an Airstrike. That's Not Such a Big Deal," *Washington Post* (9 May 2019).

- Jason Healey and Robert Jervis, "The Escalation Inversion and Other Oddities of Situational Cyber Stability," *Texas National Security Review*, Vol. 3, No. 4 (Fall 2020), pp. 30-53.
- Martin C. Libicki, "Correlations Between Cyberspace Attacks and Kinetic Attacks," *2020 12th International Conference on Cyber Conflict* (26-29 May 2020), pp. 199-213.
- Ben Buchanan and Fiona S. Cunningham, "Preparing the Cyber Battlefield: Assessing a Novel Escalation Risk in a Sino-American Crisis," *Texas National Security Review*, Vol. 3, No. 4 (Fall 2020), pp. 54-81.
- Philipp M. Lutscher, "Digital Retaliation? Denial-of-Service Attacks after Sanction Events," *Journal of Global Security Studies*, Advance Articles (2021), pp. 1-11.
- Erica D. Lonergan and Shawn W. Lonergan, "Cyber Operations, Accommodative Signaling, and the De-Escalation of International Crises," *Security Studies*, Vol. 31, No. 1 (2022), pp. 32-64.
    - Brandon K. Yoder, et al., "Cyber Operations and Signaling: An Exchange," *Security Studies*, Vol. 31, No. 4 (2022), pp. 757-789.
- Erica D. Lonergan, "The Cyber-Escalation Fallacy," *Foreign Affairs* (15 April 2022).
- Marcelo M. Leal and Paul Musgrave, "Hitting Back or Holding Back in Cyberspace: Experimental Evidence Regarding Americans' Responses to Cyberattack," *Conflict Management and Peace Sciences*, Vol. 40, No. 1 (2022), pp. 42-64.
- Ryan Shandler, Michael L. Gross, and Daphna Canetti, "Cyberattacks, Psychological Distress, and Military Escalation: An Internal Meta-Analysis," *Journal of Global Security Studies*, Vol. 8, No. 1 (2023), pp. 1-19.
- Kathryn Hedgecock and Lauren Sukin, "Responding to Uncertainty: The Importance of Covertness in Support for Retaliation to Cyber and Kinetic Attacks," *Journal of Conflict Resolution*, OnlineFirst (2023), pp. 1-31.

Session 9 (30 Oct.): Cyber Espionage (*Policy Memo #2 Due*)

Key Concepts & Discussion Questions:

- Key Concepts: espionage; cyber espionage; (passive) collection; covert operations; human intelligence (HUMINT); signals intelligence (SIGINT); Solar Winds hack; OPM hack.
- Why is it commonly argued that cyber technology will allow America's rivals to catch up quickly in military technology, often described as "death by a thousand cuts"?
- Why is the difficulty distinguishing cyber exploitation and cyber attack a problem? How should operational preparation of the environment (OPE) be classified?
- Why are U.S. advantages so great in cyber espionage?
- Why, according to Gilli and Gilli, has China has not caught up yet, despite its active cyber espionage program? Do you agree?
- China argues that economic and political espionage are no different. The U.S. argues they are. Who is right?

Required Readings (~139 pages):

- Gary D. Brown, "Spying and Fighting in Cyberspace: What is Which?" *Journal of National Security Law & Policy*, Vol, 8 (2016), pp. 621-635 (GWU library link).
- Ben Buchanan, *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics* (Cambridge: Harvard University Press, 2020), Chs. 1, 4 (On Blackboard).

- Andrea Gilli and Mauro Gilli, "Why China has not Caught Up Yet: Military-Technological Superiority and the Limits of Imitation, Reverse Engineering, and Cyber Espionage," *International Security*, Vo. 43, No. 3 (Winter 2018/19), pp. 141-189 (GWU library link).
- Brendan I. Koerner, "Inside the Cyberattack That Shocked the U.S. Government," *Wired* (23 October 2016) (External link or on Blackboard).
- **Listen:** Dina Temple-Raston, "A 'Worst Nightmare' Cyberattack: The Untold Story of the Solar Winds Hack," *NPR* (16 April 2021) (External link).

Recommended Readings:

- Thomas Rid, *Cyber War Will Not Take Place* (New York: Oxford University Press, 2013), Ch. 5.
- Adam Segal, *Hacked World Order: How States Fight, Trade, Maneuver, and Manipulate in the Digital Age* (New York: Public Affairs, 2016), Ch. 5.
- Michael P. Fischerkeller and Richard J. Harknett, "Cyber Persistence, Intelligence Contests, and Strategic Competition" *Texas National Security Review*, Special Issue: *Cyber Competition* (Fall 2020), pp. 57-73.
- Ben Buchanan, *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics* (Cambridge: Harvard University Press, 2020), Chs. 2-3, 5.
- Jon R. Lindsay, "Cyber Conflict vs. Cyber Command: Hidden Dangers in the American Military Solution to a Large-Scale Intelligence Problem," *Intelligence and National Security*, Vol. 36, No. 2 (2021), pp. 260-278.
- Amy B. Zegart, *Spies, Lies, and Algorithms: The History and Future of American Intelligence* (Princeton: Princeton University Press, 2022), pp. 251-276 (Ch. 10).

Session 10 (6 Nov.): Conventional Military Operations & Cyberspace

Key Concepts & Discussion Questions:

- Key Concepts: military cyber operation (MCO); cyber-enabled warfare; intelligence, surveillance, and reconnaissance (ISR); information operations.
- What are some of the ways in which cyber operations can play a role in conventional military operations at the strategic, operational, and tactical levels?
- What does the evidence presented by Kostyuk and Zhukov suggest about the influence of cyber operations on conventional military operations?
- What kinds of restraints and strategic dilemmas are associated with cyber technology in conventional war, according to Rovner? Do you agree?
- In what specific ways did cyber operations play a role in the Russia-Georgia War of 2008?
- In what specific ways are cyber operations playing a role in the Russia-Ukraine War (2014-)?
- In what specific ways did cyber operations play a role in the U.S. war against ISIS in Iraq and Syria?

Required Readings (~82 pages):

- Trey Herr and Drew Herrick, "Understanding Military Cyber Operations," in Richard M. Harrison and Trey Herr, eds., *Cyber Insecurity: Navigating Perils of the Next Information Age* (Lanham: Rowman & Littlefield, 2016), pp. 259-276 (On Blackboard).

- *Joint Publication 3-12: Cyberspace Operations* (Washington: Joint Chiefs of Staff, June 2018), ***only*** pp. II-9 to II-14 (start at "5. The Joint Functions and Cyberspace Operations") (On Blackboard).
- Adam Segal, *Hacked World Order: How States Fight, Trade, Maneuver, and Manipulate in the Digital Age* (New York: Public Affairs, 2016), pp. 66-78 (On Blackboard).
- Nadiya Kostyuk and Yuri M. Zhukov, "Invisible Digital Front: Can Cyber Attacks Shape Battlefield Events?" *Journal of Conflict Resolution*, Vol. 63, No. 2 (2019), pp. 317-347 (GWU library link).
- **Listen:** Dina Temple-Raston, "How the U.S. Hacked ISIS," *NPR* (26 September 2019) (External link).
- Joshua Rovner, "Warfighting in Cyberspace," *War on the Rocks* (17 March 2021) (External link).
- Thomas Rid, "Why You Haven't Heard About the Secret Cyberwar in Ukraine," *The New York Times* (18 March 2022) (External link).

Recommended Readings:

- Arthur K. Cebrowski and John J. Gartzka, "Network-Centric Warfare: Its Origin and Future," *Proceedings*, Vol. 124, No. 1 (January 1998), pp. 28-35.
- Eneken Tikk, Kadri Kaska, and Liis Vihul, *International Cyber Incidents: Legal Considerations* (Tallinn: Cooperative Cyber Defense Centre of Excellence, 2010), pp. 66-90.
- Thomas G. Mankhen, "Cyberwar and Cyber Warfare," in Kristen M. Lord and Travis Sharp, eds., *America's Cyber Future: Security and Prosperity in the Information Age*, Vol. II (Washington: Center for a New American Security, 2011), pp. 55-64.
- David Hollis, "Cyberwar Case Study: Georgia 2008," *Small Wars Journal* (January 2011), pp. 1-10.
- Ronald J. Deibert, Rafal Rohozinski, and Masashi Crete-Nishihata, "Cyclones in Cyberspace: Information Shaping and Denial in the 2008 Russia-Georgia War," *Security Dialogue*, Vol. 43, No. 1 (2012), pp. 3-24.
- Andreas Hagen, "The Russo-Georgian War 2008," in Jason Healey, ed., *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012* (Washington: The Atlantic Council, 2013), pp. 194-204.
- James A. Lewis, "'Compelling Opponents to Our Will': The Role of Cyber Warfare in Ukraine," in Kenneth Geers, ed., *Cyberwar in Perspective: Russian Aggression Against Ukraine* (Tallin: CCDCOE, 2015), pp. 39-47.
- Martin Libicki, "The Cyber War that Wasn't," in Kenneth Geers, ed., *Cyberwar in Perspective: Russian Aggression Against Ukraine* (Tallin: CCDCOE, 2015), pp. 49-54.
- Edwin Grohe, "The Cyber Dimensions of the Syrian Civil War: Implications for Future Conflict," *Comparative Strategy*, Vol. 34, No. 2 (2015), pp. 133-148.
- Adam Segal, *Hacked World Order: How States Fight, Trade, Maneuver, and Manipulate in the Digital Age* (New York: Public Affairs, 2016), Ch. 7.
- David E. Sanger, *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age* (New York: Crown, 2018), pp. 244-248.
- Thomas Zeitzoff, "Does Social Media Influence Conflict? Evidence from the 2012 Gaza Conflict," *Journal of Conflict Resolution*, Vol. 61, No. 1 (2018), pp. 29-63.
- John Arquilla, *Bitzkrieg: The New Challenge of Cyberwarfare* (Cambridge: Polity, 2021), Ch. 3.
- Nadiya Kostyuk and Aaron Brantly, "War in the Borderland Through Cyberspace: Limits of Defending Ukraine Through Interstate Cooperation," *Contemporary Security Policy*, Vol. 43, No. 4 (2022), pp. 498-515.

- Lennart Maschmeyer and Nadiya Kostyuk, "There is no Cyber 'Shock and Awe': Plausible Threats in the Ukrainian Conflict," *War on the Rocks* (8 February 2022) (External link).
- Nadiya Kostyuk and Erik Gartzke, "Why Cyber Dogs Have Yet to Bark Loudly in Russia's Invasion of Ukraine," *Texas National Security Review*, Vol. 5, No. 3 (Summer 2022), pp. 113-126 (External link).
- Erica D. Lonergan and Maggie Smith, "Want Better Cyber Policy? Talk to Social Scientists," Modern War Institute (21 July 2022) (External link).
- Marcus Willett, "The Cyber Dimensions of the Russia-Ukraine War," *Survival*, Vol. 64, No. 5 (2022), pp. 7-26.
- Nadiya Kostyuk and Erik Gartzke, "Fighting in Cyberspace: Internet Access and the Substitutability of Cyber and Military Operations," *Journal of Conflict Resolution*, OnlineFirst (2023), pp. 1-28.
- "The Evolution of Cyber Operations in Armed Conflict," *Digital Frontlines* (25 May 2025) (External link).

Session 11 (13 Nov.): Nuclear Weapons & Electoral Intervention in Cyberspace

Key Concepts & Discussion Questions:

- Key Concepts: counterproliferation; left of launch; nuclear command, control, and communications (NC3).
- What does the Israeli air strike against the Syrian Al-Kibar reactor in 2007 suggest about the relationship between cyber capabilities and nuclear weapons?
- What does the possible U.S. "left of launch" program against North Korean missiles in 2016 suggest about the relationship between cyber capabilities and nuclear weapons?
- What are some of the ways Acton argues that cyber attacks could contribute to inadvertent nuclear escalation? Is this a major concern?
- Should the United States continue to pursue counterproliferation via cyber operations?
- Should the United States continue to leave open the possibility of responding to a major cyber attack with nuclear weapons?
- How did Russia use cyber tools to intervene in the 2016 U.S. Presidential election? What were the effects of the intervention?

Required Readings (~98 pages):

- Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to do About It* (New York: Ecco, 2010), pp. 1-8 (On Blackboard).
- David E. Sanger, *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age* (New York: Crown, 2018), 268-279 (On Blackboard).
- James M. Acton, "Cyber Warfare & Inadvertent Escalation," *Daedalus*, Vol. 149, No. 2 (Spring 2020), pp. 133-149 (GWU Library link).
- David E. Sanger and William J. Broad, "Pentagon Suggests Countering Devastating Cyberattacks with Nuclear Arms," *New York Times* (16 January 2018) (External link).
- Robert S. Mueller, III, *Report on the Investigation into Russian Interference in the 2016 Election* (Washington: U.S. Department of Justice, March 2019), ***only*** pp. 1-2, 14-51 (External link).
- Michael Tomz and Jessica L. P. Weeks, "Public Opinion and Foreign Electoral Intervention," *The American Political Science Review*, Vol. 114, No. 3 (2020), pp. 856-873 (GWU library link).

Recommended Readings:

- Andrew Futter, *Hacking the Bomb: Cyber Threats and Nuclear Risks* (Washington: Georgetown University Press, 2018), Ch. 2.
- Erik Gartzke and Jon R. Lindsay, "The Cyber Commitment Problem and the Destabilization of Nuclear Deterrence," in Herbert Lin and Amy Zegart, eds., *Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations* (Washington: Brookings Institution Press, 2019), pp. 195-234.
- David C. Gompert and Martin Libicki, "Cyber War and Nuclear Peace," *Survival*, Vol. 61, No. 4 (August-September 2019), pp. 45-62.
- Herbert Lin, "Cyber Risk Across the U.S. Nuclear Enterprise," *Texas National Security Review*, Vol. 4, No. 3 (Summer 2021), pp. 107-120.
- Herbert Lin, *Cyber Threats and Nuclear Weapons* (Stanford: Stanford University Press, 2021).
- Leonard Spector, "Cyber Offense and the Changing Strategic Paradigm," *The Washington Quarterly*, Vol. 45, No. 1 (Spring 2022), pp. 38-56.
- Diego A. Martin, Jacob N. Shapiro, and Julia G. Ilhardt, "Introducing the Online Political Influence Efforts dataset," *Journal of Peace Research*, Online First (2022), pp. 1-9.

Reminder (20 Nov.): No Class (Thanksgiving Break)

Session 12 (27 Nov.): Mobilization, Repression, & Cybercrime

Key Concepts & Discussion Questions:

- Key Concepts: liberation technology; information and communications technology (ICT); China's Great Firewall; digital autocracy.
- Why has information technology been seen by many as a "liberation technology"?
- Can you think of cases that don't fit the "liberation technology" narrative—societies with high levels of internet penetration that are non-democratic? What might be going on?
- Why have some argued that information technology is a "repression technology"?
- What do Rød and Weidmann's results suggest about the relationship between the internet and democratization?
- According to King, Pan, and Roberts, what appears to be China's strategy for censorship online?
- Why do Kendall-Taylor, Franz, and Wright argue that the internet has increased autocratic durability?
- How is artificial intelligence (AI) aiding surveillance and suppression?
- In what ways does the North Korean government use the internet to perpetuate its regime?

Required Readings (~90 pages):

- Larry Diamond, "Liberation Technology," *Journal of Democracy*, Vol. 21, No. 3 (July 2010), pp. 69-83 (GWU library link).
- Espen Geelmuyden Rød and Nils B. Weidmann, "Empowering Activists or Autocrats? The Internet in Authoritarian Regimes," *Journal of Peace Research*, Vol. 52, No. 3 (2015), pp. 338-351 (GWU library link).

- Gary King, Jennifer Pan, Margaret E. Roberts, "How Censorship in China Allows Government Criticism but Silences Collective Expression" *American Political Science Review*, Vol. 107, No. 2 (May 2013), pp. 326-343 (GWU library link).
- Andrea Kendall-Taylor, Erica Frantz, and Joseph Wright, "The Digital Dictators: How Technology Strengthens Autocracy," *Foreign Affairs*, Vol. 99, No. 2 (March/April 2020), pp. 103-115 (GWU library link).
- ***Listen or read:*** Ed Caesar, "The Incredible Rise of North Korea's Hacking Army," *The New Yorker* (19 April 2021) (External link and On Blackboard).

Recommended Readings:

- Ronald Deibert and Rafal Rohozinski, "Liberation vs. Control: The Future of Cyberspace," *Journal of Democracy*, Vol. 21, No. 4 (October 2010), pp. 43-57.
- Clay Shirky, "The Political Power of Social Media: Technology, The Public Sphere, and Political Chance," *Foreign Affairs*, Vol. 90, No. 1 (February 2011), pp. 28-41.
- Evgeny Morozov, *The Net Delusion: The Dark Side of Internet Freedom* (New York: Public Affairs, 2011).
- Henry Farrell, "The Consequences of the Internet for Politics" *Annual Review of Political Science*, Vol. 15 (2012), pp. 35-52.
- Ron Deibert, "Authoritarianism Goes Global: Cyberspace Under Siege," *Journal of Democracy*, Vol. 26, No. 3 (July 2015), 64-78.
- Seva Gunitsky, "Corrupting the Cyber Commons: Social Media as a Tool of Autocratic Stability," *Perspective on Politics*, Vol. 13, No. 1 (March 2015), pp. 42-54.
- Victor Asal, Jacob Mauslein, Amanda Murdie, Joseph Young, Ken Cousins, and Chris Bronk, "Repression, Education, and Politically Motivated Cyberattacks," *Journal of Global Security Studies*, Vol. 1, No. 3 (2016), pp. 235-247.
- Joshua A. Tucker, Yannis Theocharis, Margaret E. Roberts, and Paolo Barberá, "From Liberation to Turmoil: Social Media and Democracy," *Journal of Democracy*, Vol. 28, No. 4 (October 2017), pp. 45-59.
- William R. Hobbs and Margaret E. Roberts, "How Sudden Censorship Can Increase Access to Information," *American Political Science Review*, Vol. 112, No. 3 (2018), pp. 621-636.
- Anita R. Gohdes, "Studying the Internet and Violent Conflict," *Conflict Management and Peace Science*, Vol. 35, No. 1 (2018), pp. 89-106.
- Eli Berman, Joseph H. Felter, and Jacob N. Shapiro, *Small Wars, Big Data: The Information Revolution in Modern Conflict* (Princeton: Princeton University Press, 2018), pp. 82-108 (Ch. 4).
- Ronald J. Deibert, "The Road to Digital Unfreedom: Three Painful Truths About Social Media," *Journal of Democracy*, Vol. 30, No. 1 (January 2019), pp. 25-39.
- Philipp Lutscher, Nils B. Weidmann, Margaret E. Roberts, Mattjis Jonker, Alistair King, and Alberto Dainotti, "At Home and Abroad: The Use of Denial-of-Service Attacks During Elections in Nondemocratic Regimes," *Journal of Conflict Resolution*, Vol. 64, No. 2-3 (2020), pp. 373-401.
- Anita Gohdes, "Repression Technology: Internet Accessibility and State Violence," *American Journal of Political Science*, Vol. 64, No. 3 (July 2020), pp. 488-503.
- Tiberiu Dragu and Yonatan Lupu, "Digital Authoritarianism and the Future of Human Rights," *International Organization*, Vol. 75, No. 4 (Fall 2021), pp. 991-1017.

- Denis Stukal, et al., "Why Botter: How Pro-Government Bots Fight Opposition in Russia," *The American Political Science Review*, Vol. 116, No. 3 (2022), pp. 843-857.
- Paulo Barberá, Anita R. Gohdes, Evgeniia Iakhnis, and Thomas Zeitzoff, "Distract and Divert: How World Leaders Use Social Media During Contentious Politics," *The International Journal of Press/Politics*, OnlineFirst (May 2022), pp. 1-27.
- Henry Farrell, Abraham Newman, and Jeremy Wallace, "Spirals of Delusion: How AI Distorts Decision-Making and Makes Dictators More Dangerous," *Foreign Affairs*, Vol. 101, No. 5 (September/October 2022), pp. 161-181.
- Ronald J. Deibert, "The Autocrat in Your iPhone: How Mercenary Spyware Threatens Democracy," *Foreign Affairs*, Vol. 102, No. 1 (January/February 2023), pp. 72-88.

Session 13 (4 Dec.): Norms & the Laws of Armed Conflict in Cyberspace

Key Concepts and Discussion Questions:

- Key Concepts: norms; Article 2(4) (UN Charter); Article 42 (UN Charter); Article 51 (UN Charter); laws of armed conflict; customary international law; sovereignty; *jus in bello*; *jus ad bellum*; principle of humanity; principle of necessity; principle of proportionality; principle of distinction; Tallinn Manual; retorsion
- What characteristics make a norm more likely to spread, according to Finnemore?
- What are the key stages of norm cultivation, according to Finnemore?
- What are other examples of norms that would be worth aiming to establish regarding conflict in cyberspace?
- Under what conditions do cyber activities constitute a use of force under international law? Where should the line between force and non-force in cyberspace be drawn?
- What are some of the characteristics of cyberspace that make the application of international law difficult, according to Brown and others?

Required Readings (72 pages):

- Martha Finnemore, "Cultivating International Cyber Norms," in Kristen M. Lord and Travis Sharp, eds., *America's Cyber Future: Security and Prosperity in the Information Age*, Vol. II (Washington: Center for a New American Security, 2011), pp. 87-102 (On Blackboard).
- Joseph S. Nye, Jr., "The End of Cyber-Anarchy? How to Build a New Digital Order," *Foreign Affairs*, Vol. 101, No. 1 (January/February 2022), pp. 32-42 (GWU library link).
- Harold Hongju Koh, "International Law in Cyberspace," *Harvard International Law Journal*, Online Vol. 54 (December 2012), pp. 1-12 (External link).
- Michael N. Schmitt, "The Law of Cyber Targeting," *Naval War College Review*, Vol. 68, No. 2 (Spring 2015), pp. 1-20 (GWU library link).
- Gary D. Brown, "International Law and Cyber Conflict," in Eneken Tikk and Mika Kerttunen, *Routledge Handbook of International Cybersecurity* (London: Routledge, 2020), pp. 366-378 (On Blackboard).

Recommended Readings:

- Herbert S. Lin, "Offensive Cyber Operations and the Use of Force," *Journal of National Security Law & Policy*, Vol. 63, No. 4 (2010), pp. 63-86.

- Michael N. Schmitt, "Cyber Operations and the Jus Ad Bellum Revisited," *Villanova Law Review*, Vol. 56, No. 3 (2011), pp. 569-606.
- Eneken Tikk, "Ten Rules for Cyber Security," *Survival*, Vol. 53, No. 3 (June-July 2011), pp. 119-132.
- Matthew C. Waxman, "Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)," *Yale Journal of International Law*, Vol. 36, No. 2 (2011), pp. 421-459.
- Mary Ellen O'Connell, "Cyber Security without Cyber War," *Journal of Conflict & Security Law*, Vol. 17, No. 2 (2012), pp. 187-209.
- Henry Farrell, "Promoting Norms for Cyberspace" *Council on Foreign Relations Cyber Brief* (April 2015).
- Martha Finnemore and Duncan B. Hollis, "Constructing Norms for Global Cybersecurity," *The American Journal of International Law*, Vol. 110 (2017), pp. 425-479.
- Michael N. Schmitt, ed., *The Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (New York: Cambridge University Press, 2017), Pts. III-IV.
- Alex Grigsby, "The End of Cyber Norms," *Survival*, Vol. 59, No. 6 (December 2017-January 2018), pp. 109-122.
- Lucas Kello, "Cyber Threats," in Thomas G. Weiss and Sam Daws, eds., *The Oxford Handbook on the United Nations* (New York: Oxford University Press, 2018).
- Sergei Boeke and Dennis Broeders, "The Demilitarisation of Cyberconflict," *Survival*, Vol. 60, No. 6 (December 2018-January 2019), pp. 73-90.
- Michael N. Schmitt, "Taming the Lawless Void: Tracking the Evolution of International Law Rules for Cyberspace," *Texas National Security Review*, Vol. 3, No. 3 (Autumn 2020), pp. 32-47.
- Michael J. Mazarr, "Virtual Territorial Integrity: The Next International Norm," *Survival*, Vol. 62, No. 4 (August-September 2020), pp. 101-118.
- Rhiannon Neilsen, "Coding protection: 'cyber humanitarian interventions' for preventing mass atrocities," *International Affairs*, Vol. 99, No. 1 (2023), pp. 299-319.

Session 14 (11 Dec.): Review & The Future of Conflict in Cyberspace

Key Concepts and Discussion Questions:

- Key Concepts: artificial intelligence; quantum technology
- What is artificial intelligence and how does it relate to international security?
- What are some potential dangers in the development of AI?
- What is quantum technology and how does it relate to international security?

Required Readings (~23 pages):

- Paul Scharre, "Killer Apps: The Real Dangers of an AI Arms Race," *Foreign Affairs*, Vol. 98, No. 3 (May/June 2019), pp. 135-144 (GWU library link).
- Michael J. Biercuk and Richard Fontaine, "The Leap into Quantum Technology: A Primer for National Security Professionals," *War on the Rocks* (17 November 2017) (External link).

Recommended Readings:

- Michael C. Horowitz, "Artificial Intelligence, International Competition, and the Balance of Power," *Texas National Security Review*, Vol. 1, No. 3 (May 2018), pp. 36-57.
- Paul Scharre, *Army of None: Autonomous Weapons and the Future of War* (New York: W.W. Norton & Co., 2018), pp. 211-230 (Ch. 14).
- Christian Brose, *The Kill Chain: Defending America in the Future of High-Tech Warfare* (New York: Hachette, 2020), pp. 118-140 (Ch. 7).
- Michael C. Horowitz, et al., "Policy Roundtable: Artificial Intelligence and International Security," *Texas National Security Review* (02 June 2020), pp. 1-52.
- Jon R. Lindsay, "Demystifying the Quantum Threat: Infrastructure, Institutions, and Intelligence Advantage," *Security Studies*, Vol. 29, No. 2 (2020), pp. 335-361.
- Jon R. Lindsay, "Surviving the Quantum Cryptocalypse," *Strategic Studies Quarterly*, Vol. 14, No. 2 (Summer 2020), pp. 49-73.
- Avi Goldfarb and Jon R. Lindsay, "Prediction and Judgment: Why Artificial Intelligence Increases the Importance of Humans in War," *International Security*, Vol. 46, No. 3 (Winter 2021/22), pp. 7-50.
- Michael C. Horowitz, Lauren Kahn, and Laura Resnick Samotin, "A Force for the Future: A High-Reward, Low-Risk Approach to AI Military Innovation," *Foreign Affairs*, Vol. 101, No. 3 (May/June 2022), pp. 157-164.
- Henry Farrell, Abraham Newman, and Jeremy Wallace, "Spirals of Delusion: How AI Distorts Decision-Making and Makes Dictators More Dangerous," *Foreign Affairs*, Vol. 101, No. 5 (September/October 2022), pp. 168-181.
- Ben Buchanan and Andrew Imbrie, *The New Fire: War, Peace, and Democracy in the Age of AI* (Cambridge: MIT Press, 2022).

18 December 2023, 11:59:59 PM: Policy Paper Due

Policies

Incomplete Grades

At the option of the instructor, an Incomplete may be given for a course if a student, for reasons beyond the student's control, is unable to complete the work of the course, and if the instructor is informed of, and approves, such reasons before the date when grades must be reported. An Incomplete can only be granted if the student's prior performance and class attendance in the course have been satisfactory. Any failure to complete the work of a course that is not satisfactorily explained to the instructor before the date when grades must be turned in will be graded F, Failure.

If acceptable reasons are later presented to the instructor, the instructor may initiate a grade change to the symbol I, Incomplete. The work must be completed within the designated time period agreed upon by the instructor, student, and school, but no more than one calendar year from the end of the semester in which the course was taken. To record the exact expectations, conditions, and deadlines of the Incomplete please use the Elliott School's Incomplete Grade Contract:

Incomplete Grade Contract for Graduate Courses

The completed and signed contract is to be submitted to the Academic Affairs and Student Services Office. All students who receive an Incomplete must maintain active student status during the subsequent semester(s) in which the work of the course is being completed. If not registered in other classes during this period, the student must register for continuous enrollment status. For more information regarding Incompletes please review the relevant sections in the University Bulletin:

http://bulletin.gwu.edu/university-regulations/#graduatetext

Instructor Response Time

I will usually respond to emails within 24 hours, often considerably faster. On weekends, I may be somewhat slower. If you haven't heard back from me via email within 24 hours, please feel free to follow up.

I will return graded assignments within one week.

Statement on Inclusive Teaching

In support of inclusive excellence, the Elliott School is committed to supporting our faculty and students in exercising inclusive teaching throughout our curriculum. All faculty members are expected to practice inclusive teaching as outlined in ESIA inclusive teaching statement (https://elliott.gwu.edu/statement-inclusive-teaching) and to include a stated commitment in the syllabus. Resources for inclusive teaching can be found here: https://elliott.gwu.edu/inclusive-teaching-resources.

Differences in time Zone

All the times in this course correspond to the U.S. Eastern Time zone (e.g., Washington, DC). It is your responsibility to convert these times to the time zone of your location so that you can meet this course's deadlines.

Inclement Weather

In-person classes may be held online in case of inclement weather. Faculty will inform students of relevant instructional continuity plans.

Late Work

Late submissions of assignments will be deducted one letter gradient (e.g., A to A-, A- to B+, etc.) for each day they are late. Extensions will be granted on a case-by-case basis for illnesses, family emergencies, religious observances, and the like. If you are seeking an extension for one of these reasons, please give me as much advance notice as is possible. Extensions will rarely be granted on or in the day or two leading up to a due date, except under extraordinary circumstances.

GW Acceptable Use for Computing Systems and Services

All members of the George Washington University must read and comply with the Acceptable Use Policy when accessing and using computing systems and services, including email and Blackboard. Please read the Acceptable Use Policy to familiarize yourself with how GW information systems are to be used ethically.

Academic Integrity

Academic dishonesty is defined as cheating of any kind, including misrepresenting one's own work, taking credit for the work of others without crediting them and without appropriate authorization, and the fabrication of information. Note that using artificial intelligence such as ChatGPT to help write any part of any assignment is a violation of academic integrity.

Please review GW's policy on academic integrity, located at: https://studentconduct.gwu.edu/code-academic-integrity. All graded work must be completed in accordance with the George Washington University Code of Academic Integrity. For more information, see Promoting Academic Integrity.

Sharing of Course Content

Unauthorized downloading, distributing, or sharing of any part of a recorded lecture or course materials, as well as using provided information for purposes other than the student's own learning may be deemed a violation of GW's Student Conduct Code.

Use of Student Work (FERPA)

The professor will use academic work that you complete during this semester for educational purposes in this course during this semester. Your registration and continued enrollment constitute your consent.

Copyright Policy Statement

Materials used in connection with this course may be subject to copyright protection under Title 17 of the United States Code. Under certain Fair Use circumstances specified by law, copies may be made for private study, scholarship, or research. Electronic copies should not be shared with unauthorized users. If a user fails to comply with Fair Use restrictions, he/she may be liable for copyright infringement. For more information, including Fair Use guidelines, see Libraries and Academic Innovations Copyright page.

Bias-Related Reporting

At the George Washington University, we believe that diversity and inclusion are crucial to an educational institution's pursuit of excellence in learning, research, and service. Acts of bias, hate, or discrimination are anathema to the university's commitment to educating citizen leaders equipped to thrive and to serve in our increasingly diverse and global society. We strongly encourage students to report possible bias incidents. For additional information, follow this link: https://diversity.gwu.edu/bias-incident-response.

Disability Support Services & Accessibility

If you may need disability accommodations based on the potential impact of a disability, please register with Disability Support Services (DSS) at: https://disabilitysupport.gwu.edu/. If you have questions about disability accommodations, contact DSS at 202-994-8250 or dss@gwu.edu or visit them in person in Rome Hall, Suite 102.

For information about how the course technology is accessible to all learners, see the following resources:

Blackboard accessibility

Kaltura (video platform) accessibility

Voicethread accessibility

Microsoft Office accessibility

Adobe accessibility

Religious Observances

In accordance with University policy, students should notify faculty during the first week of the semester of their intention to be absent from class on their day(s) of religious observance. For details and policy, see: https://registrar.gwu.edu/university-policies#holidays.

Mental Health Services

The University's Mental Health Services offers 24/7 assistance and referral to address students' personal, social, career, and study skills problems. Services for students include: crisis and emergency mental health consultations confidential assessment, counseling services (individual and small group), and referrals. For additional information call 202-994-5300 or see: https://healthcenter.gwu.edu/counseling-and-psychological-services.

Emergency Preparedness and Response Procedures

The University has asked all faculty to inform students of these procedures, prepared by the GW Office of Public Safety and Emergency Management in collaboration with the Office of the Executive Vice President for Academic Affairs.

To Report an Emergency or Suspicious Activity

Call the University Police Department at 202-994-6111 (Foggy Bottom) or 202-242-6111 (Mount Vernon).

Shelter in Place – General Guidance

Although it is unlikely that we will ever need to shelter in place, it is helpful to know what to do just in case. No matter where you are, the basic steps of shelter in place will generally remain the same.

- If you are inside, stay where you are unless the building you are in is affected. If it is affected, you should evacuate. If you are outdoors, proceed into the closest building or follow instructions from emergency personnel on the scene.
- Locate an interior room to shelter inside. If possible, it should be above ground level and have the fewest number of windows. If sheltering in a room with windows, move away from the windows. If there is a large group of people inside a particular building, several rooms may be necessary.
- Shut and lock all windows (for a tighter seal) and close exterior doors.
- Turn off air conditioners, heaters, and fans. Close vents to ventilation systems as you are able. (University staff will turn off ventilation systems as quickly as possible).
- Make a list of the people with you and ask someone to call the list in to UPD so they know where you are sheltering and who is with you. If only students are present, one of the students should call in the list.
- Await further instructions. If possible, visit GW Campus Advisories for incident updates or call the GW Information Line 202-994-5050.

- Make yourself comfortable and look after one other. You will get word as soon as it is safe to come out.

Evacuation

An evacuation will be considered if the building we are in is affected or we must move to a location of greater safety. We will always evacuate if the fire alarm sounds. In the event of an evacuation, please gather your personal belongings quickly (purse, keys, GWorld card, etc.) and proceed to the nearest exit. Every classroom has a map at the door designating both the shortest egress and an alternate egress. Anyone who is physically unable to walk down the stairs should wait in the stairwell, behind the closed doors. Firemen will check the stairwells upon entering the building.

Once you have evacuated the building, proceed to our primary rendezvous location: the court yard area between the GW Hospital and Ross Hall. In the event that this location is unavailable, we will meet on the ground level of the Visitors Parking Garage (I Street entrance, at 22nd Street). From our rendezvous location, we will await instructions to re-enter the School.

Alert DC

Alert DC provides free notification by e-mail or text message during an emergency. Visit GW Campus Advisories for a link and instructions on how to sign up for alerts pertaining to GW. If you receive an Alert DC notification during class, you are encouraged to share the information immediately.

GW Alert

GW Alert provides popup notification to desktop and laptop computers during an emergency. In the event that we receive an alert to the computer in our classroom, we will follow the instructions given. You are also encouraged to download this application to your personal computer. Visit GW Campus Advisories to learn how.

Additional Information

Additional information about emergency preparedness and response at GW or the University's operating status can be found on GW Campus Advisories or by calling the GW Information Line at 202-994-5050.