Carnegie Mellon University

Remote Systems and the Cyber Domain in Conflict

Tuesday/Thursday, 11:00am-12:20pm, Wean Hall (WEH) 5403

Course Number: 84-387 / 84-687

Instructor Information

Name	Josh Schwartz
Contact Info	joshschwartz@cmu.edu
Office Location / Hours	Posner Hall 370; Tuesday 1:00-3:00pm or By Appointment

TA Information

Name	Sydney Boyer
Contact Info	sjboyer@andrew.cmu.edu
Office Location / Hours	Zoom; Friday 1:00-2:00pm or By Appointment

What Is This Course About?

For most of human history, warfare took place face-to-face or in close proximity using weapons like rocks, swords, spears, bow and arrows, and firearms. However, the development of technologies like missiles, drones, and the internet have changed the character of warfare by enabling actors to use lethal force and cause disruption thousands of miles away from the battlefield. Technological advancements have arguably even led to the creation of an entirely human-made domain of warfare—the cyber domain—that is distinct from the land, sea, air, and space domains. This course will analyze the impact of drones and the cyber domain on international conflict. In particular, we will study the historical origins of these technologies, why and how they have spread, their use and effectiveness on the battlefield, ethical questions surrounding their use, and whether arms control is possible. How is the information revolution in computing similar and different from prior revolutions in military affairs? Are drones and the cyber domain transforming conflict by giving the offense a significant advantage over the defense, or is their offensive and destructive potential exaggerated? Is coercion possible in cyberspace, or does the "attribution problem" impede deterrence? Might drones actually reduce the risks of escalation in interstate conflict by removing the desire for revenge if a pilot is killed? Does the possibility of cyberwar increase the risks of nuclear weapons being used? How has the internet been weaponized to enable economic warfare and election interference? Might cyber espionage undermine the United States' military advantage, and should the US ban TikTok? Do drones decrease or increase terrorism? Is remote warfare and the use of lethal autonomous weapons systems—sometimes referred to as killer robots—inherently unethical? These are just a handful of the questions we will explore in this class. By the end of the course, students will have a grasp of the history of the information revolution and many of the key debates and theories in this field.

Learning Objectives

1. Articulate key debates and questions related to the role of remote systems and cyber tools in the domain of international conflict. Be able to make a reasoned argument for one side of a debate or another.
2. Analyze key policy questions related to remote systems and the cyber domain in international conflict, and be able to make specific, implementable policy recommendations based on a reasoned consideration of the medium and long-term historical dynamics associated with an issue.
3. Explain the historical development of the technologies underlying remote systems and the cyber domain in conflict, as well as how they have been used.
4. Describe alternative perspectives on whether arms control is possible, the ethics of conducting warfare from a distance, etc., and formulate personal viewpoints
5. Apply political science theories to explain the factors that impact the spread of these technologies.
6. Evaluate the effectiveness of these technologies and the scale of their impact on international politics.
7. Hone writing, research, speaking, and analytical skills that are valuable for any career.

Assignments/Grading

In-Class Participation (10%)

I hope you will learn something from me over the course of the semester, but just as importantly I believe you will learn much from each other (and I will learn from you). However, this requires that you attend and actively participate in class. Participation includes asking questions, answering questions I ask the class as a whole, and being active in small group work. Although this is a bigger class, if I don't know you by the end of the semester or you're not frequently participating, then you'll lose out on these easy points.

Policy Pitch Presentation (10%) and Written Policy Memo (20%)

Pick one session of the course (e.g., the class on the spread of drones). Your goal will be to make a policy recommendation about a *contemporary* international relations issue or debate related in some way to the topic of that class. For example, for the class on the spread of drones, you could write about how the US (or any other country / international organization!) can better control the spread of drones by enacting regulations, creating international agreements, modifying its drone export policy, and so on. For the class on whether the offense has the advantage in the cyber domain, you could write about how the US or Ukraine should (or should not) use cyber-attacks against Russia. For the class on economic warfare, you could write about when sanctions should be used or how they can be implemented more effectively. If you are unsure about whether an idea meets these criteria, please reach out to me.

How Do I Sign Up for a Topic/Class? You can access the sign-up sheet here or on Canvas under "Pages" and "Policy Memo/Presentation Sign-Up Sheet." Click "edit" at the top of the page and add your name. *The deadline to sign up is January 25*. Only a certain number of people will be allowed to choose each class session, and so act fast.

Policy Pitch Presentation: After picking a topic, the first thing you will do is give a policy pitch presentation on the day class meets for the session you chose. Your presentation should address five questions: (1) Who is the audience for this policy presentation? Pick a relevant person that has some influence over the issue in question. For example, a president or prime minister, secretary of state or defense, senator or member of congress, military leader, head of an international organization, or director of a human rights group. Pretend you are actually briefing this person and stay in character. (2) What is the problem with current policy (i.e., the status quo)? In other words, explain why the current policy isn't working and why some kind of change is needed. Use statistics and/or real-world examples to answer this question. (3) Why is this an important issue that the person you are briefing should care about / devote time and energy to? (4) What is your policy recommendation(s)? In other words, how would you *change* current policy to address the problem? Your policy recommendation(s) should be feasible and reasonably specific. (5) What do you anticipate will be the major criticisms of your policy recommendation, and why should we dismiss those criticisms or how does your policy recommendation address them? *The presentation should be 5 minutes or less (strictly enforced) and should be thought of as a kind of Shark Tank pitch in that every detail need not be included in the presentation*. After your presentation, be prepared for questions and suggestions from your classmates and me. You may use slides if you prefer (email them to me at least two hours before class), but you do not have to. If you do use slides, make sure you're not just reading off of them.

Written Policy Memo: The person you gave the policy pitch presentation to is intrigued and has now asked you to write a formal, more in-depth policy memo. The memo is due 7 days after you give the policy pitch presentation (e.g., if you present on Tuesday, then the memo should be submitted on Canvas by 11:59pm at the latest the following Tuesday). The memo can and should be updated in response to the feedback you received from the policy pitch presentation. This can include revising or even significantly changing your policy recommendation(s). The memo should be between 1,250 and 2,000 words (about 5-8 pages double-spaced). Use Chicago style *footnotes* to cite your sources. These footnotes do *not* count towards the word limit and there's no need for a separate bibliography section. Your memo should include at least six sections. First, three lines ("to," "from," and "regarding") that say who the memo is to, who it is from, and what it is regarding. Second, an executive summary section that very briefly (in one paragraph) explains what the contemporary problem is, why it matters, and what your principal recommendation(s) are (this does not contribute to the world limit). Third, a section on the problem with current policy. Fourth, a section on why this is an important issue. Fifth, a section outlining your specific policy recommendation(s) (e.g., "policy recommendation 1," "policy recommendation 2," etc.). You need not make more than one policy recommendation, but you can if you want to. In this section, discuss how challenges related to adoption (e.g., getting Congress or the United Nations to adopt this policy change) and implementation will be overcome. Most importantly, in this section explain your logic for why adopting these policies is the best option to solve the problem. Sixth, a section on the likely criticisms of your policy recommendation(s). In this section, "steel-man" (rather than "straw-man") your actual or hypothetical opponents. Explain why we should dismiss these criticisms or how your policy recommendations address them (e.g., perhaps you include certain qualifications in your policy proposal or conditions where you recommend policy should be abandoned). Seventh, a short conclusion section that reminds the decision-maker you're trying to convince of the bigger-picture and what the consequences would be if they don't adopt your recommendations. Where appropriate, try and reference course readings and concepts (especially the readings for the class session you're focused on) to inform your analysis.

Reading Quizzes (30%)

Cramming before midterms or finals is counter-productive to learning because (a) that means you cannot effectively participate in class discussion, and (b) research has shown that information studied in a cramming session is less likely to be remembered in the long-term. To provide a bit of an incentive or "nudge" for you to do the reading each week, we'll start most Thursday classes (unless otherwise noted on the syllabus) with a short (5 minute) closed-note quiz. The questions will be focused on the readings from that Tuesday and Thursday. They will mostly consist of multiple choice, true/false questions, and (very) short answer questions. The questions are not meant to trick you! My goal in designing the quizzes is that if you did the reading, you should average an A over the course of the semester. And because we're doing quizzes, we will not have any midterm exams or an *in-class* final. If you want to take quizzes on your computer, please download Respondus LockDown Browser (instructions are on the last page).

Final Essay (30%)

The final exam will be a take-home essay assignment. Students will be given a set of essay questions and will choose two topics to write short (about 5 pages double-spaced) essays on. The expectation is that students will cite readings and concepts from the course in order to answer the essay questions. Outside research will not be required. The final exam questions will be released on April 19 and the exam will be due on April 26 at 11:59pm on Canvas. When we get closer to the end of the semester, I will give you more details about the exam.

Grading Scale

Undergraduate Students: A (90-100%), B (80-89%), C (70-79%), D (60-69%) R (under 60%).

Graduate Students: A (93-100%), A- (90-92%), B+ (87-89%), B (83-86%), B- (80-82%), C+ (77-79%), C (73-76%), C- (70-72%), D+ (77-79%), D (63-66%), D- (60-62%), R (under 60%).

Missing Class / Late Assignments Due to Extenuating Circumstances

Attending and participating in class discussions helps facilitate learning; not only for you, but also for your peers. Therefore, part of your grade is based on your attendance and active participation. Turning in assignments on time is also important for ensuring that no student(s) have an unfair advantage. It's also good practice for your future job. With that being said, your health, wellness, religious beliefs, professional advancement, etc. is important to me and I recognize you may occasionally need to miss class or turn in an assignment late due to extenuating circumstances. This includes (but isn't limited to) a physical or mental health crisis, family medical emergency, religious event, or job interview. If you need to miss class or cannot turn in an assignment on time due to one of these issues, then please *let me know at least 48 hours in advance* (except in the case of an emergency) and we can find an appropriate accommodation. In the case of unexcused late assignments, 5% will be taken off for each 24 hours late.

Overview of the Class Schedule

There are four main parts of the course and each sub-bullet point below reflects a topic we will spend a class discussing.

- **Part I: Historical Background and the Basic Fundamentals of Computing**
  - War Before the Information Revolution — A History of Military Revolutions
  - Historical Origins of the Information Revolution and How the Internet Works
  - The Revolution's Watershed Moment? The Case of the Gulf War
- **Part II: Proliferation**
  - Drone Proliferation to State and Non-State Actors — Supply and Demand
  - The Spread of Cyber Panic and Cyber Military Institutions — The Role of Popular Culture and Language
- **Part III: Use and Effectiveness**
  - Conventional, Interstate Conflict
    - What Factors Increase the Chance of War? Offense-Defense Theory and the Impact of Technology
    - The Debate Over Whether Drones Favor the Offense
    - Does Offense have the Advantage in the Cyber Domain? The Case of the Stuxnet Cyber Attack on Iran's Nuclear Program
    - Winning Without Actually Using Force — The Fundamentals of Coercion Theory and Application to Drones
    - The Debate about Whether Coercion is Possible in the Cyber Domain
    - Escalation Dynamics — Public and Policymaker Support for Retaliation
  - Nuclear, Interstate Conflict
    - Judgement Day? The Cyber Domain and the Risk of Nuclear War
  - Guest Speaker: The Dog That Didn't Bark? The Limited Effectiveness of Cyber Attacks in the Russia-Ukraine War
  - Non-Military, Interstate Conflict
    - Weaponized Interdependence — Economic Warfare and the Internet
    - An Arrow at the Heart of Democracy? Hacking, Social Media Information Operations, and Election Interference
    - Is Cyber *War* the Wrong Analogy? Intelligence Contests, Cyber Espionage of Military Secrets, and the Debate Over Banning TikTok
  - Use By and Against Non-State Actors
    - Power to the People? The Role of Terrorist Groups, Hacktivists, and CEOs
    - Guest Speaker: The Role of Commercial Actors — Dual Use Technologies, Public-Private Partnerships, and Autonomous Aerial Drones
    - The Debate Over Whether Drones Increase or Decrease Terrorism — The Pessimistic Argument
    - The Debate Over Whether Drones Increase or Decrease Terrorism — The Optimistic Argument
    - The Drone Debate at the Cinema — Eye in the Sky
- **Part IV: Controlling Use — Ethics and Arms Control**
  - Is Controlling Drones and Cyber Capabilities Possible?
  - Is Remote Warfare Inherently Unethical? The Morality of Killing from a Distance
  - Are Killer Robots an Ethical Abomination, or a Moral Imperative?
  - Guest Speaker: The Legitimacy of Drone Warfare — Public Opinion and International Law

Detailed Class Schedule

All readings are available for free as PDFs. Access them here or by going to the course Canvas page and navigating to the "Files" section.

January 16: Introduction to the Course

- Suggested Reading
  - Joseph S. Nye Jr., "Cyber Power," *Harvard Kennedy School* (2010), Link, Only pages 1-9.
  - Lucas Kello, "The Meaning of the Cyber Revolution," *International Security* (2013), Link, Only pages 17-22.
  - Michael P. Kreuzer, "Cyberspace is an Analogy, Not a Domain," *Strategy Bridge* (2021), Link, 7 pages.
  - Rubrick Biegon et al., "Remote Warfare — Buzzword or Buzzkill?" *Defence Studies* (2021), Link, Only pages 430-433.
- Key Questions
  - What are remote systems and what is remote warfare? How "remote" do you need to be to count as remote warfare, and what are the elements of remoteness?
  - What is the cyber domain and cyber warfare?
  - Do you agree with the argument that there is a cyber "domain" distinct from the land, air, sea, and space domains?
  - Why should we care about this topic?

PART I: Historical Background and the Basic Fundamentals of Computing

January 18: War Before the Information Revolution — A History of Military Revolutions

- Required Reading
  - Andrew F. Krepinevich, "From Cavalry to Computer: The Pattern of Military Revolutions," *The National Interest* (1994), Link, Only pages 30-middle of page 40.
  - Jacquelyn Schneider, "The Capability-Vulnerability Paradox and Military Revolutions: Implications for Computing, Cyber, and the Onset of War," *Journal of Strategic Studies* (2019), Link, 16 pages.
- Key Questions
  - What have been the key military-technological revolutions throughout history?
  - What is the capability-vulnerability paradox?
  - How does the cyber domain and remote systems differ from prior military revolutions? How are they similar?
  - What lessons can we learn from prior military revolutions? How do they relate to our current era of warfare dominated by information/computing technologies?
- No Quiz

January 23: Historical Origins of the Information Revolution and How the Internet Works

- Required Reading
  - Max Boot, *War Made New: Technology, Warfare, and the Course of History, 1500 to Today*, "The Rise of the Information Age," Gotham (2006), Access on Canvas, Only pages 307-313.
  - P.W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know*, "Part I: How It All Works," Oxford University Press (2014), Link, Only pages 12-55 and 60-66.
- Key Questions
  - What roles did government and private actors play in developing computers and the internet?
  - How does the internet work? What are its vulnerabilities?
  - Are the vulnerabilities the internet introduces made worth it by the benefits of connection?

January 25: The Revolution's Watershed Moment? The Case of the Gulf War

- Required Reading
  - Keith L. Shimko, *The Iraq Wars and America's Military Revolution*, Cambridge University Press (2012), Link, Only pages 1-3 and 53-90.
  - Roundtable on Keith Shimko's *The Iraq Wars and America's Military Revolution*, "Review by Jasen J. Castillo," H-Diplo/ISSF (2013), Link, *Only* pages 7-10 in the pdf.
- Key Questions
  - Why was the outcome of the 1991 Gulf War viewed by many as so shocking?
  - What information revolution technologies were key to the American-led coalition's victory in the Gulf War?
  - How important was technology to the US' victory? What alternative explanations (besides technology) are there for the outcome of the conflict?
- Quiz

PART II: Proliferation

January 30: Drone Proliferation to State and Non-State Actors — Supply and Demand

- Required Reading
  - Michael C. Horowitz et al., "China Has Made Drone Warfare Global," *Foreign Affairs* (2020), Link, 6 pages.
  - Andrea Gilli and Mauro Gilli, "The Diffusion of Drone Warfare? Industrial, Organizational, and Infrastructural Constraints," *Security Studies* (2016), Link, Only pages 51-60 and 71-76.
  - Audrey Kurth Cronin, *Power to the People: How Open Technological Innovation is Arming Tomorrow's Terrorists*, Oxford University Press (2020), Link, Only pages 1-4, 12-15, 203-219, and 223-226.
  - Kerry Chávez and Ori Swed, "The Proliferation of Drones to Violent Nonstate Actors," *Defence Studies* (2021), Link, Only pages 1-5.
  - Greg Myre, "A Chinese Drone for Hobbyists Plays a Crucial Role in the Russia-Ukraine War," *NPR* (2023), Link.

- Key Questions
  - What role does regime type play in the spread of drones to state actors?
  - Should the United States have a more or less liberal export policy when it comes to the sale of armed drones to other countries?
  - What are some of the key challenges associated with arms control when it comes to drone proliferation to state and non-state actors?
  - What kinds of drones are non-state actors (e.g., terrorist groups) most likely to acquire? Why?
  - What role are commercial drones playing in the Russia-Ukraine War?

February 1: The Spread of Cyber Panic and Cyber Military Institutions –– The Role of Popular Culture and Language

- Required Reading
  - Kevin Bankston, "How Sci-Fi Like 'WarGames' Led to Real Policy During the Reagan Administration," *New America* (2018), Link, 4 pages.
  - Sean T. Lawson, *Cybersecurity Discourse in the United States: Cyber-Doom Rhetoric and Beyond*, "The Sky is Falling! An Introduction to Cyber-Doom," Routledge (2019), Link, Only pages 1-8.
  - Nicholas Goldberg, "The Never-Ending Obfuscation of War," *Los Angeles Times* (2022), Link, 5 pages.
    - Note: This reading is to get you thinking about how language impacts our understanding of the world. The next two readings will apply this to the cyber domain.
  - Jordan Branch, "What's in a Name? Metaphors and Cybersecurity," *International Organization* (2021), Link, 24 pages.
  - Myriam Dunn Cavelty, "From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse," *International Studies Review* (2013), Link, Only pages 110-111.
- Key Questions
  - Can movies and popular culture influence government policy and how we think about policy issues? If so, then why and how do they have an impact?
  - What are the ways in which language, metaphors, and analogies impact how we view cyber issues specifically and political issues more broadly? What are some key examples?
- Quiz

PART III: Use and Effectiveness

A. Conventional, Interstate Conflict

February 6: What Factors Increase the Chance of War? Offense-Defense Theory and the Impact of Technology

- Required Reading
  - Sean M. Lynn-Jones, "Offense-Defense Theory and Its Critics," *Security Studies* (1995), Link, 31 pages.
  - Keir A. Lieber, "Grasping the Technological Peace: The Offense-Defense Balance and International Security," *International Security* (2000), Link, Only pages 77-85.

- Key Questions
  - What does offense-defense theory predict with respect to the likelihood of war and the chance of arms control?
  - Can weapons be effectively classified as offensive or defense?
  - Does it matter if subjective perceptions of the overall offense-defense balance don't match the objective reality?
  - Which are the features of technologies that are commonly believed to impact whether they advantage the offense or the defense to a greater extent?
  - Can offense-defense theory explain the dynamics of critical conflicts, such as World War I, World War II, and the Cold War?
  - How important is technology to explaining the offense-defense balance compared to other variables?

February 8: The Debate Over Whether Drones Favor the Offense

- Required Reading
  - Jason Lyall, "Drones Are Destabilizing Global Politics: Simple Vehicles Make Conflict Tempting and Cheap," *Foreign Affairs* (2020), Link, 4 pages.
  - Antonio Calcara et al., "Why Drones Have Not Revolutionized War: The Enduring Hider-Finder Competition in Air Warfare," *International Security*, Link, Only pages 130-139, 143-144, 147, bottom of 149-153, 161-165, and 169-171.
  - Paul Lushenko and Sarah Kreps, "Tactical Myths and Perceptions of Reality," *Security Studies* (2023), Link, 8 pages.
  - Jacquelyn Schneider, "Unscorable at 12: Technically Correct, But Misses the Mark," *Security Studies*, Link, 7 pages.
- Key Questions
  - What is Calcara et al.'s argument for why drones have not revolutionized warfare and don't provide the offense a significant advantage? What evidence do they point to?
  - What are the key criticisms of Calcara et al.'s argument?
  - On balance, do you believe drones favor the offense or defense? By how much?
- Quiz

February 13: Does Offense have the Advantage in the Cyber Domain? The Case of the Stuxnet Cyber Attack on Iran's Nuclear Program

- Required Reading
  - Ilai Saltzman, "Cyber Posturing and the Offense-Defense Balance," *Contemporary Security Policy* (2013), Link, Only pages 42-45.
  - Lucas Kello, "The Meaning of the Cyber Revolution," *International Security* (2013), Link, Only pages 27-32.
  - Jon R. Lindsay, "Stuxnet and the Limits of Cyber Warfare," *Security Studies* (2013), Link, Only pages 365-369, 375-384, and 385-396.
  - Rebecca Slayton, "What is the Cyber Offense-Defense Balance?" *International Security* (2017), Link, Only pages 82-86 and 97-104.
- Key Questions
  - According to Saltzman, how should the variables of firepower and mobility, which are often key to the arguments made by proponents of offense-defense theory, be revised to fit the context of cyber warfare?

- What are the arguments and evidence for why the cyber domain may give the offense an advantage? Why might playing defense in cyber space be difficult?
- What are the arguments and evidence for why the cyber domain may give the defense an advantage or, at least, not give the offense much of an advantage?
- Which perspective of the debate does the Stuxnet cyber attack support in your view?

February 15: Winning Without Actually Using Force — The Fundamentals of Coercion Theory and Application to Drones

- *Required Reading*
  - Tami Davis Biddle, "Coercion Theory: A Basic Introduction for Practitioners," *Texas National Security Review* (2020), Link, Only pages 95-106.
  - Stephen Van Evera, "The Spiral Model v. The Deterrence Model," *MIT* (1997), Link, 4 pages.
  - Michael Horowitz and Dan Reiter, "When Does Aerial Bombing Work?" *Journal of Conflict Resolution* (2001), Link, Only pages 150-153.
  - Amy Zegart, "Cheap Flights, Credible Threats: The Future of Armed Drones and Coercion," *Journal of Strategic Studies* (2020), Link, *Only* pages 6-12 and 15-31.
  - Kelly A. Grieco and J. Wesley Hutto, "Can Drones Coerce?" *International Politics* (2023), Link, Only pages 932-933.
  - Michael Horowitz et al., "Separating Fact from Fiction in the Debate over Drone Proliferation," *International Security* (2016), Link, Only pages 31-32.
  - Robert A. Pape, "Why Airpower Cannot Salvage Russia's Doomed War in Ukraine," *Foreign Affairs* (2022), Link, Only page 2-5 of the pdf.
- Key Questions
  - What is the difference between coercion and brute force? What are the advantages of utilizing the former rather than the latter?
  - What is the difference between deterrence and compellence? Which is harder?
  - What are the prerequisites for coercion to succeed?
  - What is the difference between the spiral and deterrence model? How can the spiral model explain the potential failure of strategic bombing strategies used against civilian populations in conflicts like World War II and the Russia-Ukraine War?
  - In what ways is it harder to use drones rather than other military technologies for coercion, and what coercive advantages might drones provide? Which perspective do you find most convincing?
- Quiz

February 20: The Debate about Whether Coercion is Possible in the Cyber Domain

- Required Reading
  - Erica D. Borghard and Shawn W. Lonergan, "The Logic of Coercion in Cyberspace," *Security Studies* (2017), Link, Only pages 452-459, 471-475, and 477-478.
  - Erik Gartzke, "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth," *International Security* (2013), Link, Only pages 41-43 and 58-63.
  - Emily Tamkin, "10 Years After the Landmark Attack on Estonia, Is the World Better Prepared for Cyber Threats?" *Foreign Policy* (2017), Link, 4 pages.

    - Joseph S. Nye Jr., "Deterrence and Dissuasion in Cyberspace," *International Security* (2017), Link, Only pages 44-46, bottom of 49-52, and 55-62.
    - Nadiya Kostyuk, "Deterrence in the Cyber Realm: Public versus Private Cyber Capacity," *International Studies Quarterly* (2021), Link, Only pages 1151-1153 and 1158-1160.
    - Julian E. Barnes, "Cyber Command Operation Took Down Russian Troll Farm for Midterm Elections," *New York Times* (2019), Link, 2 pages.
- Key Questions
    - In what ways is it difficult to use the threat of cyber attacks to coerce adversaries, and what coercive advantage might cyber tools provide? Which perspective do you find most convincing?
    - In what ways is it difficult to deter the use of cyber attacks by an adversary against you? What role does the "attribution problem" play?
    - In what ways can cyber attacks be deterred? For example, what is the impact of public cyber institutions?
    - How does the 2007 cyber attack against Estonia illustrate these dynamics?

February 22: Escalation Dynamics –– Public and Policymaker Support for Retaliation

- Required Reading
    - Erik Lin-Greenberg, "Wargame of Drones: Remotely Piloted Aircraft and Crisis Escalation," *Journal of Conflict Resolution* (2022), Link, 21 pages.
    - Erik Lin-Greenberg, "Evaluating Escalation: Conceptualizing Escalation in an Era of Emerging Military Technologies," *Journal of Politics* (2023), Link, 5 pages.
    - 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* (2023), Link, Only pages 1874, bottom of 1877-1879, and 1894-1895.
    - Erica D. Lonergan and Shawn W. Lonergan, *Escalation Dynamics in Cyberspace*, "The U.S. Dogs That Didn't Bark," *Oxford University Press* (2023), Link, Only pages 115-129.
- Key Questions
    - How are the escalation dynamics associated with shooting down a drone different from those when an inhabited aircraft is shot down?
    - Compared to other technologies, how does the use of drones and cyber attacks impact the likelihood of escalation?
    - What role does uncertainty play in impacting the chances of escalation? How does this relate to the "attribution problem" previously discussed in the course?
    - How do you compare the value of experimental wargames conducted on military officers versus experiments conducted on national security experts versus experiments conducted on the general public?
    - Should the US have escalated further in response to Chinese hacking? What about in response to the downing of an expensive drone by Iran?
- Quiz

B. Nuclear, Interstate Conflict

February 27: Judgement Day? The Cyber Domain and the Risk of Nuclear War

- Required Reading
  - Nicholas Thompson, "Inside the Apocalyptic Soviet Doomsday Machine," *Wired* (2009), Link.
  - Dylan Matthews, "40 Years Ago Today, One Man Saved Us from World-Ending Nuclear War," *Vox* (2023), Link.
  - Herbert Lin, "Cyber Risk Across the U.S. Nuclear Enterprise," *Texas National Security Review* (2021), Link, Only pages 109-113 and 115.
  - Jacquelyn Schneider et al., "Hacking Nuclear Stability: Wargaming Technology, Uncertainty, and Escalation," *International Organization* (2023), Link, Only pages 633-639, 641-646, and 651-662.
- Key Questions
  - What was Dead Hand/Perimeter? Do you believe the use of such a system is wise? How does it impact the effectiveness of nuclear deterrence?
  - What did Stanislav Petrov do? Did he make the right decision, and would you have made a similar decision if in his shoes?
  - What are the cyber vulnerabilities associated with the US nuclear weapons arsenal?
  - What are the different impacts that technological certainty and uncertainty can have on the likelihood of nuclear stability?
  - What do Schneider et al. find is the greatest threat to nuclear stability? Is their evidence convincing?

February 29: The Dog That Didn't Bark? The Limited Effectiveness of Cyber Attacks in the Russia-Ukraine War

- GUEST SPEAKER: Naidya Kostyuk
  - Assistant Professor, School of Public Policy and the School of Cybersecurity and Privacy at the Georgia Institute of Technology
  - PhD, University of Michigan
  - One of the top experts on cyber war and the political dimensions of cyber conflict
- Required Reading
  - Nadiya Kostyuk and Erik Gartzke, "Why Cyber Dogs Have Yet to Bark Loudly in Russia's Invasion of Ukraine," *Texas National Security Review* (2022), Link, 13 pages.
  - Nadiya Kostyuk and Yuri M. Zhukov, "Invisible Digital Front: Can Cyber Attacks Shape Battlefield Events?" *Journal of Conflict Resolution* (2019), Link, Only pages 318-322, bottom of 333, 336-337, and 340-341 (i.e., you can skip the statistical models if you want).
- Assignment: Post two questions for Nadiya on Canvas under the "Discussions" section (see here)
- No Quiz

March 5: NO CLASS (Spring Break)

March 7: NO CLASS (Spring Break)

C. Non-Military, Interstate Conflict

March 12: Weaponized Interdependence —– Economic Warfare and the Internet

- Required Reading
  - Henry Farrell and Abraham L. Newman, "Weaponized Interdependence: How Global Economic Networks Shape State Coercion, *International Security* (2019), Link, 38 pages.
  - Henry Farrell and Abraham L. Newman, "How the U.S. Stumbled Into Using Chips as a Weapon Against China," *Wall Street Journal* (2023), Link, 6 pages.
- Key Questions
  - What are the theoretical ways in which interdependence can reduce the probability of conflict?
  - How can interdependence be "weaponized" to enable conflict? What role does the internet play in enabling weaponization?
  - How are countries—–especially targets of these attacks—–reacting?
  - Should the United States and other countries exploit interdependence to engage in economic warfare generally? What about in the specific cases of punishing Russia for their invasion of Ukraine or combatting China?

March 14: An Arrow at the Heart of Democracy? Hacking, Social Media Information Operations, and Election Interference

- Required Reading
  - Dov H. Levin, "When the Great Power Gets a Vote: The Effects of Great Power Electoral Interventions on Election Results," *International Studies Quarterly* (2016), Link, 13 pages.
  - Richard J. Harknett and Max Smeets, "Cyber Campaigns and Strategic Outcomes," *Journal of Strategic Studies* (2022), Link, Only pages 534-535.
  - Abigail Abrams, "Here's What We Know So Far About Russia's 2016 Meddling," *TIME* (2019), Link.
  - Michael Tomz and Jessica L.P. Weeks, "Public Opinion and Foreign Electoral Intervention," *American Political Science Review* (2020), Link, 16 pages.
- Key Questions
  - How successful has electoral interference been historically, and what are the two conditions Levin argues make interference more likely to occur and be effective?
  - What does Russia's intervention in the 2016 election indicate about the "attribution problem" when it comes to cyber attacks?
  - How can cyber operations be used strategically rather than just tactically? In which category should we put Russia's 2016 intervention in the election?
  - What are the key public opinion dynamics associated with electoral intervention, especially those related to partisanship and military retaliation?
  - Should the United States have responded more forcefully to Russia's 2016 intervention?
- Quiz

March 19: Is Cyber *War* the Wrong Analogy? Intelligence Contests, Cyber Espionage of Military Secrets, and the Debate Over Banning TikTok

- Required Reading
  - Joshua Rovner, "Cyber War as an Intelligence Contest," *War on the Rocks* (2019), Link, 8 pages.
  - 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* (2019), Link, Only pages 141-144, 149-152, and 178-186.
  - Shahryar Pasandideh et al., "Correspondence: Military-Technological Imitation and Rising Powers," *International Security* (2019), Link, Only pages 187-192.
  - Sapna Maheshwari and Amanda Holpuch, "Why Countries Are Trying to Ban TikTok," *New York Times* (2023), Link, 4 pages.
  - Fareed Zakaria, "Why Banning TikTok Won't Do Any Good," *Washington Post* (2023), Link, 2 pages.
- Key Questions
  - What are the key features of cyber intelligence contests?
  - How severe is the threat of cyber espionage of defense secrets? What are the arguments and evidence for why it's a major threat versus a minor threat?
  - What are the arguments for and against banning TikTok? Who do you think is right?

D. Use By and Against Non-State Actors

March 21: Power to the People? The Role of Terrorist Groups, Hacktivists, and CEOs

- Required Reading
  - Michael J. Boyle, *The Drone Age: How Drone Technology Will Change War and Peace*, "Chapter 5: Terrorist Drones," Oxford University Press (2020), Link, Only pages 1-7 of the pdf.
  - Zachary Kallenborn, "Why Cheap Drones Pose a Significant Chemical Terrorism Threat," *Bulletin of the Atomic Scientists* (2023), Link, 4 pages.
  - Tom Donilon, "The Drone Threat Comes Home: Time to Wake Up to a Growing Domestic Danger," *Foreign Affairs* (2022), Link, Only pages 4-8 of the pdf.
  - Adam Satariano et al., "Elon Musk's Unmatched Power in the Stars," *New York Times* (2023), Link, 20 pages.
  - Tim Maurer, "Cyber Proxies and their Implications for Liberal Democracies," *The Washington Quarterly* (2018), Link, Only pages 171-179.
  - William Akoto, "Accountability of Cyber Conflict: Examining Institutional Constraints on the Use of Cyber Proxies," *Conflict Management and Peace Science* (2022), Link, Only pages 313-315.
  - Matt Burgess, "Ukraine's Volunteer 'IT Army' Is Hacking in Uncharted Territory," *Wired* (2022), Link, 4 pages.
- Key Questions
  - In what ways have drones been used by terrorist groups? What are some of the potential commercial targets terrorist groups could attempt to use drones to attack?
  - What are some potential solutions to the use of commercial drones by terrorist groups? How big a difference do you think they'd make?

    - What is the military and strategic importance of satellites, and why are some concerned about the control that individuals like Elon Musk have over them?
    - What are the different types of cyber proxies, and what kinds of activities do they engage in? What role have they played in the Russia-Ukraine War?
- Quiz

March 26: The Role of Commercial Actors — Dual Use Technologies, Public-Private Partnerships, and Autonomous Aerial Drones

- GUEST SPEAKER: Marcel Bergerman
    - Chief Operating Officer (COO) and Co-Founder of Near Earth Autonomy
    - PhD, Carnegie Mellon University
    - Previously faculty at CMU's Robotics Institute
    - Near Earth Autonomy is a Pittsburgh-based company that is developing autonomous aerial drones. They have developed autonomous drones that can deliver blood to the frontlines to help injured soldiers, been awarded contracts by the US military, and recently won the Pittsburgh Technology Council's 2022 Innovator of the Year Award
- Assignment: Post two questions for Marcel on Canvas under the "Discussions" section (see here). Peruse Near Earth Autonomy's website to learn more.

March 28: The Debate Over Whether Drones Increase or Decrease Terrorism — The Pessimistic Argument

- Required Reading
    - Michael J. Boyle, "The Costs and Consequences of Drone Warfare," *International Affairs* (2013), Link, Only pages 1-4 and 7-13.
    - Richard Wike et al., "Global Opposition to U.S. Surveillance and Drones, But Limited Harm to America's Image," *Pew* (2014), Link, Only pages 4-6.
    - Anouk S. Rigterink, "Drone Dilemma: The Risks of Washington's Favorite Counterterrorism Tool Often Outweigh the Rewards," *Foreign Affairs* (2021), Link, 4 pages.
    - Zach Beauchamp, "The Entire Basis for Obama's Drone Strategy May Be Wrong," *Vox* (2014), Link, 5 pages.
    - "Living Under Drones: Death, Injury, and Trauma to Civilians from US Drone Practices in Pakistan," *Stanford Law School International Human Rights and Conflict Resolution Clinic / NYU School of Law Global Justice Clinic* (2012), Link, Only pages v-viii, 55-62, 74-76, and 80-88.
- Key Questions
    - What are the different mechanisms by which drone strikes could end up increasing rather than decreasing terrorism?
    - What are principal-agent problems, and how might they cause drone strikes to increase terrorism? How does this argument relate to our previous discussion of cyber proxies?
    - How does the strength of a terrorist group's bureaucracy impact its susceptibility to leadership decapitation using drones or other methods?
    - What are the physical and psychological impact of drones on civilians in targeted areas?
- Quiz

April 2: The Debate Over Whether Drones Increase or Decrease Terrorism — The Optimistic Argument

- Required Reading
  - Patrick B. Johnson and Anoop K. Sarbahi, "The Impact of US Drone Strikes on Terrorism in Pakistan," *International Studies Quarterly* (2016), Link, Only pages 203-207.
  - Asfandyar Mir and Dylan Moore, "Drones, Surveillance, and Violence: Evidence from a US Drone Program," *International Studies Quarterly* (2019), Link, Only pages 846-848.
  - Bryce Loidolt, "Managed Risks, Managed Expectations: How Far Will Targeted Killings Get the United States in Afghanistan?" *War on the Rocks* (2021), Link, 6 pages.
  - Aqil Shah, "Drone Blowback: Much Ado about Nothing?" *Lawfare* (2018), Link, 4 pages.
  - Neha Ansari, "Precise and Popular: Why People in Northwest Pakistan Support Drones," *War on the Rocks* (2022), Link, 8 pages.
  - Joshua A. Schwartz and Matthew Fuhrmann, "Do Armed Drones Reduce Terrorism? Here's the Data," *Washington Post* (2022), Link, 2 pages.
  - Avery Plaw and Matthew S. Fricker, "Tracking the Predators: Evaluating the US Drone Campaign in Pakistan," *International Studies Perspectives* (2012), Link, Only pages 350-354.
- Key Questions
  - What are the differences between kinetic effects (aka degradation) and anticipatory effects (aka disruption effects)?
  - What does an analysis of al-Qaeda documents recovered from the operation that killed Osama Bin Laden reveal about the effectiveness of drones? How convincing is this evidence?
  - How do drone optimists combat the argument that drones cause "blowback" among civilian populations, potentially increasing the number of people willing to join or help terrorist organizations?
  - How does the risk of civilian casualties differ when drones are used compared to other types of military technologies or operations?
  - On balance, do you believe drone pessimists or optimists make the more compelling argument?

April 4: The Drone Debate at the Cinema — Eye in the Sky

- Required Reading: None

PART IV: Controlling Use — Ethics and Arms Control

April 9: Is Controlling Drones and Cyber Capabilities Possible?

- Required Reading
  - Eric Lipton, "As A.I.-Controlled Killer Drones Become a Reality, Nations Debate Limits," *New York Times* (2023), Link, 5 pages.
  - Jane Vaynman and Tristan A. Volpe, "Dual Use Deception: How Technology Shapes Cooperation in International Relations," *International Organization* (2023), Link, 30 pages.
  - Erica D. Borghard and Shawn W. Lonergan, "Why Are There No Cyber Arms Control Agreements?" *Council on Foreign Relations* (2018), Link, 4 pages.
- Key Questions
  - How does the dual use nature of a technology impact the likelihood of arms control?
  - What role do the factors of "distinguishability" and "integration" play?
  - Is arms control likely in the cyber domain or with respect to drones?
  - If arms control was possible, would pursuing it be wise?
- No Quiz

April 11: NO CLASS (Spring Carnival)

April 16: Is Remote Warfare Inherently Unethical? The Morality of Killing from a Distance

- Required Reading
  - Quinta Jurecic, "Moral Theory and Drone Warfare," *Lawfare* (2015), Link, 6 pages.
  - John Brennan, "The Efficacy and Ethics of U.S. Counterterrorism Strategy," *Wilson Center* (2012), Link, Only pages 12-17.
    - Note: This was a speech by a government official in the Obama Administration who eventually became director of the CIA
  - Bradley Jay Strawser, "Moral Predators: The Duty to Employ Uninhabited Aerial Vehicles," *Journal of Military Ethics* (2010), Link, Only pages 343-345.
  - Paul W. Kahn, "The Paradox of Riskless Warfare," *Philosophy & Public Policy Quarterly* (2002), Link, 7 pages.
  - Robert Sparrow, "Riskless Warfare Revisited: Drones, Asymmetry and the Just Use of Force," in *Ethics of Drone Strikes*, Edinburgh University Press (2021), Link, Only pages 15-20.
  - John Kaag and Sarah Kreps, "The Moral Hazard of Drones," *New York Times* (2012), Link, 6 pages.
  - Dave Philipps, "The Unseen Scars of Those Who Kill Via Remote Control," *New York Times* (2022), Link, 5 pages.
  - Christopher M. Faulkner and Jeff Rogg, "Ten Years After the Al-Awlaki Killing: A Reckoning for the United States' Drone Wars Awaits," *Modern War Institute at West Point* (2021), Link, 9 pages.
  - Jack L. Goldsmith, "A Just Act of War," *New York Times* (2011), Link, 4 pages.
- Key Questions
  - What are the principles of discrimination, proportionality, and necessity? Do drones make it easier or harder to abide by these principles?

- What are the arguments for why killing by remote control is inherently unethical? For example, what is Kaag/Kreps' argument related to moral hazard and Kahn's argument related to killing from a distance?
- If killing from a distance with drones is unethical, is killing from a distance with aircraft, missiles, and artillery also immoral?
- What are the arguments for why killing by remote control is either not unethical or a moral imperative? For example, what is the principle of unnecessary risk (PUR)?
- What are the legal, moral, and practical arguments for and against assassinating a US citizen without any judicial trial? Was killing Anwar al-Awlaki justified or not?
- On balance, do you believe killing by remote control from a distance is (a) inherently unethical, (b) ethical, (c) a moral imperative, or (d) it depends on the circumstances?

April 18: Are Killer Robots an Ethical Abomination, or a Moral Imperative?

- Required Reading
  - Denise Garcia, "The Case Against Killer Robots: Why the United States Should Ban Them," *Foreign Affairs* (2014), Link, 4 pages.
  - Campaign to Stop Killer Robots, "Problems with Autonomous Weapons," Link, a few pages.
  - Ronald C. Arkin, "The Case for Ethical Autonomy in Unmanned Systems," *Journal of Military Ethics* (2010), Link, Only pages 332-336.
  - Hitoshi Nasu and Christopher Korpela, "Stop the 'Stop the Killer Robot' Debate: Why We Need Artificial Intelligence in Future Battlefields," *Council on Foreign Relations* (2022), Link, 8 pages.
  - Thomas X. Hammes, "Autonomous Weapons Are the Moral Choice," *Atlantic Council* (2023), Link, 3 pages.
  - Kevin Jon Heller, "The Concept of 'The Human' in the Critique of Autonomous Weapons," *Harvard National Security Journal* (2023), Link, Only pages 6-8, bottom of 14-18, and 20-41.
- Key Questions
  - What are the arguments that lethal autonomous weapons systems (LAWS) are unethical? Especially those related to algorithmic biases and a lack of accountability.
  - What are the arguments that LAWS are ethical? In particular, why might LAWS actually reduce the incidence of civilian casualties compared the use of force more directly by humans?
  - To what extent are LAWS already used by the United States and other countries?
  - Even if we stipulate LAWS are unethical, should they still be developed and (potentially) used for strategic reasons?
  - Is killing with LAWS or by remote control from a distance more ethically problematic?
- Quiz (The last one!)

April 23: The Legitimacy of Drone Warfare —– Public Opinion and International Law

- GUEST SPEAKER: Lieutenant Colonel Paul Lushenko
  - Director of Special Operations and Faculty Instructor, U.S. Army War College Department of Military Strategy, Planning, and Operations
  - PhD, Cornell University

    - Expert on drone warfare
    - Co-Author of *The Legitimacy of Drone Warfare: Evaluating Public Perceptions*
    - Co-Editor of *Drones and Global Order: Implications of Remote Warfare for International Society*
- Required Reading: None
- Assignment: Post two questions for Paul on Canvas under the "Discussions" section (see here)

April 25: What We've Learned — The Highlights

- Required Reading: None

Questions to Ask When Evaluating Theories

- Are the concepts and variables in the theory defined clearly?
- Are the factors in the theory necessary and/or sufficient conditions for certain outcomes to occur?
- Does the author explain the *logic* of why X causes Y? Do you buy it? Are there alternative mechanisms explaining why X causes Y that the author doesn't consider?
- Does the author consider the counterfactual? If so, then does the author use counterfactuals effectively? If not, consider them yourself.
- Is the causal claim falsifiable? In other words, is there evidence that you could realistically find that would disprove the theory?
- Are there historical examples that do not conform to the author's argument? Would the theory hold in other contexts (e.g., time periods, countries, etc.)?
- What factors make the theory more and less likely to hold?
- Does the author consider rival explanations and treat them fairly?
- Might there be omitted variables bias? That is, could there be a variable correlated with both the independent and dependent variables of a theory that's the real cause?
- Could there be reverse causation? Might Y cause X rather than the other way around?

News Resources to Follow International Security Current Events

- Foreign Affairs
- War on the Rocks
- Foreign Policy
- Bulletin of the Atomic Scientists
- Lawfare

Respect, Diversity, and Inclusion

I am committed to ensuring that my classroom is a friendly and inclusive learning environment that will serve students from all diverse backgrounds and perspectives. Although I encourage rigorous debate, you should always treat each other with respect, and I commit to doing so as well. The diverse perspectives, areas of expertise, and lived experiences we bring to the classroom is something I view as a great strength that will help facilitate learning. I do not permit bullying or harassment under any circumstances. Do not hesitate to reach out to me with any concerns you may have, and there will never be any backlash of retaliation permitted for raising concerns. CMU also offers resources through the Center for Student Diversity and Inclusion.

Learning Resources Offered by CMU

CMU offers various programs via the Student Academic Success Center to support student learning outside the traditional course structure.

Mental Health Resources Offered by CMU

Taking care of your mental health, in addition to your physical health, is critically important. If you're struggling with anxiety, depression, or anything else, then I'd urge you to seek support. CMU offers Counseling and Psychological Services (CaPS). Visit their website or call them at 412-268-2922 for 24/7 support. You can also call the Re:solve Crisis Network at 888-796-8226 or the National Suicide Prevention Lifeline at 800-273-8255.

Accommodations for Students with Disabilities

If you have a disability and have an accommodations letter from the Disability Resources office, I encourage you to discuss your accommodations and needs with me as early in the semester as possible. I will work with you to ensure that accommodations are provided as appropriate. If you suspect that you may have a disability and would benefit from accommodations but are not yet registered with the Office of Disability Resources, I encourage you to contact them at access@andrew.cmu.edu.

Academic Integrity

Academic dishonesty will not be tolerated because it is antithetical to learning. See CMU's Policy on Academic Integrity for more information.

Policy on the Use of Artificial Intelligence for Assignments

Just as the internet revolutionized how students completed their assignments, generative artificial intelligence (GAI) tools—such as ChatGPT—are likely to do the same. For that reason, I don't believe a blanket ban on the use of GAI in this class is appropriate. In my view, we need to learn how to most effectively use these tools to enhance learning rather than ban them. Therefore, you may feel free to use ChatGPT to generate ideas for assignments or conduct research, *but you must cite your use of it, or it will be considered academic misconduct.* I would also strongly caution you against relying too much on ChatGPT, as it is quite prone to misstating academic arguments and historical events, as well as making up sources. While you may use ChatGPT to generate ideas or conduct research (as long as you cite it), *your writing must be your own*. Do not use ChatGPT to write your essay or memo, or that will be considered academic misconduct.

Respondus LockDown Browser

This course requires the use of LockDown Browser for online exams. Watch this video to get a basic understanding of LockDown Browser:

https://www.respondus.com/products/lockdown-browser/student-movie.shtml

Download Instructions

- Select a quiz from the course (I've posted an ungraded practice quiz on Canvas)
- If you have not already installed LockDown Browser, select the link to download the application and follow the installation instructions
- Return to the quiz page in a standard browser
- LockDown Browser will launch and the quiz will begin