GERALD R. FORD SCHOOL OF PUBLIC POLICY
UNIVERSITY OF MICHIGAN

Cybersecurity Threats and Policy Approaches

475.001/750.001

Fall 2023

Mondays/Wednesdays, 4:00pm-5:20pm EST

Instructor:	Javed Ali, Associate Professor of Practice alimust@umich.edu (email) 3227 Weill (office location) 1110 Weill (class location)
Instructor Office Hours:	Mondays/Wednesdays, 2:30pm-4:00pm EST
Course Term:	Mondays/Wednesdays, 4:000pm-5:20pm EST 15-week session 28 August 2023 – 6 December 2023

Course Description: Concerns over cybersecurity threats are no longer the sole province of the federal government and now affect virtually all spheres of society from state and local governments, the private sector, and individual citizens. Amongst the challenges that all these stakeholders must confront are a decentralized federal government architecture; different legal and policy guidelines and authorities; gaps and seams in response and prevention capabilities; a diverse array of adversaries who utilize different cyber tools and methods to conduct operations for different goals and objectives; and, a rapidly evolving technological landscape that can quickly render technical and policy solutions obsolete.

In order to enhance understanding on the complexities described above, this class will examine a variety of issues regarding cybersecurity threats and different policy approaches. The first half examines major categories of cyber threat adversaries and different tools and techniques that have been used against the United States. The second half traces the evolution of the U.S. cybersecurity policy and legal framework, delves into how the US government is currently organized around cybersecurity, and explores the strengths and weaknesses of various policy approaches. These sessions will involve a combination of lectures and student panels that explore each of these different policy topics.

Course Objectives: The objectives of the course include:

1. Assessing the diversity of the cyber threat landscape.
2. Evaluating the evolution of US cybersecurity policies and governmental frameworks.
3. Examining strengths and weaknesses of potential prevention and response options.
4. Sharpening critical thinking, executive briefing, and team collaboration skills.

Course Grading: This class encompasses several graded components to include: two policy memos of various style and format; four summaries of course themes and materials; a class presentation that involves teamwork and collaboration with other students; and,in-class participation and engagement.

Class participation	10%
Summary memos	15%
Policy assessment panels	25%
Policy memos	50%
	100%

Class participation, engagement, and attendance: Given the seminar-based format for the class, active student participation is essential in order to: a) express comprehension of assigned reading and lecture material; b) discuss current events related to cybersecurity issues; c) offer perspectives, comments, and questions about lecture content; and d) engage in cross-student discussion and reflection. This component of the class grade (10%) will be based on my assessment of student engagement in these criteria, which may include "cold-calling" on students. Instructor-directed questions to students based on submitted questions for panels, or questions about administrative or syllabus-related details, ***will not be counted as participation activity under*** this framework.

While attendance is not formally part of the participation grade, absences in class eliminate opportunities to learn, participate, and develop bonds with fellow classmates, and is something students will have to consider when not attending. **In addition, the following schema sets forth grade deductions for attendance absences without prior notification to me in writing via email.** This is a professional standard that is common in workplace environments.

0-1 unexcused absences	No grade deduction
2-3 unexcused absences	5% grade deduction
4-5 unexcused absences	10% grade deduction
6-7 unexcused absences	15% grade deduction
8-9 unexcused absences	20% grade deduction
10-11 unexcused absences	25% grade deduction
12-13 unexcused absences	30% grade deduction

Summary memos: Four summary memos that answer questions provided in the syllabus for different themes and topics will be required at 9am on modules 3, 4, 5, and 6. **Each memo will be worth 3.75% individually for a total of 15% of the class grade.** Memos will be submitted in Canvas and should consist of at least 500-600 words and answer questions based on a comprehension of assigned readings, lecture material, and any outside research. Memos will not be reviewed for grammar, style, and punctuation but rather on the basis of substantive comprehension. **Memos submitted after 9am until 12pm will be docked 25%; memos submitted after 12pm will not receive a grade since the purpose of this assignment is to think critically about relevant themes in advance and be prepared to discuss them during class.**

Summary memo #1 due 9am, Monday September 11
Summary memo #2 due 9am, Monday September 18
Summary memo #3 due 9am, Monday September 25
Summary memo #4 due 9am, Monday October 2

Student Panels: Seven student panels will be convened during **modules 9, 10, 11, 12, 14, and 15.** Students will be split into teams to provide either a "pro or con" perspective (the pro team presenting the strengths and the con team presenting the weaknesses) of select cybersecurity policy topics. The size of the pro and con teams will depend on the overall number of students in the class, and students will be assigned to the different panels and pro/con teams in each panel based on an ordinal distribution. ***As a result, students will not have a choice on which panel or which side of the pro/con debate they ultimately fall but each student will only be on one panel during the semester.***

Student panel dates & issues:

Panel #1: Wednesday, October 25
Military approaches: DoD 2023 Cyber Strategy pros/cons

Panel #2: Wednesday, November 1
Diplomatic approaches: 2021 Cyber Diplomacy Act pros/cons

Panel #3: Wednesday, November 8
Homeland security/law enforcement approaches: CISA 2024-2026 Strategic Plan pros/cons

Panel #4: Wednesday, November 15
Artificial intelligence approaches: 2021 Artificial Intelligence Commission Report pros/cons

Panel #5: Wednesday, November 29
Information-sharing approaches: Cyber Incident Reporting for Critical Infrastructure Act of 2022 pros/cons

Panel #6: Wednesday, December 6
Election security approaches: HR 2722, the SAFE Act pros/cons

Timing: Each student will have up to five to seven minutes individually to present their position via a powerpoint presentation within the pro or con team, with a maximum of 15 to 20 minutes total for each team collectively. The instructor will then pose questions to the panelists based on student submissions and other sources.

Grading: Students operating in teams will be evaluated on their oral presentation skills, adherence to the recommended presentation format, and research and preparation for their “pro” or “con” assessment. Following the panel presentations, other students in class will engage in a question-and-answer session with the assembled student panel. Approximately 15% of this grade will be determined by the student’s performance on their assigned panel and 10% (5 panels x 2%) will be based on preparation as audience members on the non-assigned panels. As an audience member, each student will submit in advance a one paragraph summary (three to four-sentences) of their “pro” or “con” position for the selected administration and at least one question via the assigned panel-specific files in Canvas at 9am the day of each panel. **Summaries submitted after 9am until 12pm will be docked 25%; those submitted after 12pm will not receive a grade since the purpose of the summaries and questions is to think critically about panel themes in advance and be prepared to discuss them during class.**

Policy Memos: Two different writing assignments will be required, with different formats, structures, and grading requirements. Collectively these will equal 50% of the total grade (25% + 25%). These memos will be due at the beginning of class on **October 11 and December 6** and submitted via memo-specific files created in Canvas. **Absent a medical or family emergency that is communicated in writing, or a documented medical accommodation form, no extensions will be granted prior the due date.** Substantively, there is no “right or wrong answer” regarding the selected topics in these two assignments. ***However, students will be evaluated in their ability to: write cogently and concisely; present a logical argument within a coherent memo structure; and minimize grammatical or spelling errors and avoid colloquial expressions.*** Students will be expected to conduct research to support their assessments beyond the material listed in the course readings, and details on all the potential issues are available through Internet-based sources from major newspapers like the *New York Times* and *Washington Post;* a variety of national security-related periodicals and websites; academic and research organizations; and U.S. government publications and documents. ***Memos will be singled-spaced in 12-point Times New Roman font, in MS Word .doc format (not Adobe .pdf format) with bolded text to designate headers between key sections and ordinal footnotes or endnotes to support factual references.***

- Policy Memo #1 (***Due at the beginning of class, Wednesday October 11***): In a four-to-five-page memo, describe the cyber threat from one of the five covered in class (Russia, China, Iran, North Korea, and hackers and criminal groups) and the methods, tools, and tactics they have used against the United States; assess how cyber operations fit within their overall national security, criminal, or ideological agenda; and, provide a single policy option that could limit the effectiveness of future operations from the selected threat.

- Policy Memo #2: (***Due at the beginning of class, Wednesday December 6)*** In a four-to-five-page memo, describe the origin, background, and major points in the selected policy document for one of the six policy approaches covered in class (military, diplomatic, homeland security/law enforcement, artificial intelligence, information-sharing, and election security); evaluate the strengths and weaknesses of the document's approach on US cybersecurity; and, provide a single policy option that could strengthen US cybersecurity in that particular policy arena.

Ford School Inclusivity Statement: Members of the Ford School community represent a rich variety of backgrounds and perspectives. We are committed to providing an atmosphere for learning that respects diversity. While working together to build this community we ask all members to:

- share their unique experiences, values and beliefs
- be open to the views of others
- honor the uniqueness of their colleagues
- appreciate the opportunity that we have to learn from each other in this community
- value one another's opinions and communicate in a respectful manner
- keep confidential discussions that the community has of a personal (or professional) nature
- use this opportunity together to discuss ways in which we can create an inclusive environment in Ford classes and across the UM community

Ford School Public Health Protection Policy: In order to participate in any in-person aspects of this course--including meeting with other students to study or work on a team project--you must follow all the public health safety measures and policies put in place by the State of Michigan, Washtenaw County, the University of Michigan, and the Ford School. Up to date information on U-M policies can be found here. It is expected that you will protect and enhance the health of everyone in the Ford School community by staying home and following self-isolation guidelines if you are experiencing any symptoms of COVID-19

Student Mental Health and Wellbeing: The University of Michigan is committed to advancing the mental health and wellbeing of its students. We acknowledge that a variety of issues, both those relating to the pandemic and other issues such as strained relationships, increased anxiety, alcohol/drug problems, and depression, can directly impact students' academic performance and overall wellbeing. If you or someone you know is feeling overwhelmed, depressed, and/or in need of support, services are available.

You may access counselors and urgent services at Counseling and Psychological Services (CAPS) and/or University Health Service (UHS). Students may also use the Crisis Text Line (text '4UMICH' to 741741) to be connected to a trained crisis volunteer. You can find additional resources both on and off campus through the University Health Service and through CAPS.

Accommodations for Students with Disabilities: If you believe you need an accommodation for a disability, please reach out to U-M Services for Students with Disabilities (SSD) office to help determine appropriate academic accommodations and how to communicate about your accommodations with your professors. Any information you provide will be treated as private and confidential.

Academic Integrity: The Ford School academic community, like all communities, functions best when its members treat one another with honesty, fairness, respect, and trust. We hold all members of our community to high standards of scholarship and integrity. To accomplish its mission of providing an optimal educational environment and developing leaders of society, the Ford School promotes the assumption of personal responsibility and integrity and prohibits all forms of academic dishonesty, plagiarism and misconduct. Academic dishonesty may be understood as any action or attempted action that may result in creating an unfair academic advantage for oneself or an unfair academic advantage or disadvantage for any other member or members of the academic community. Plagiarism involves representing the words, ideas, or work of others as one's own in writing or presentations, and failing to give full and proper credit to the original source. Conduct, without regard to motive, that violates the academic integrity and ethical standards will result in serious consequences and disciplinary action. The Ford School's policy of academic integrity can be found in the MPP/MPA, BA, and PhD Program handbooks. Additional information regarding academic dishonesty, plagiarism and misconduct and their consequences is available at: http://www.rackham.umich.edu/current-students/policies/academic-policies/section11#112

Use of Technology: Students should follow instructions from their instructor as to acceptable use of technology in the classroom, including laptops, in each course. All course materials (including slides, assignments, handouts, pre-recorded lectures or recordings of class) are to be considered confidential material and are not to be shared in full or part with anyone outside of the course participants. Likewise, your own personal recording (audio or video) of your classes or office hour sessions is allowed only with the express written permission of your instructor. If you wish to post course materials or photographs/videos of classmates or your instructor to third-party sites (e.g. social media), you must first have informed consent. ***Without explicit permission from the instructor and in some cases your classmates, the public distribution or posting of any photos, audio/video recordings or pre-recordings from class, discussion section or office hours, even if you have permission to record, is not allowed and could be considered academic misconduct.***

Please review additional information and policies regarding academic expectations and resources at the Ford School of Public Policy at: https://intranet.fordschool.umich.edu/academic-expectations

SYLLABUS

Module 1 – August 28 & August 30 — Course Overview and Introduction to Cybersecurity

Summary: This module introduces foundational concepts on cybersecurity and provides a roadmap for how the course will flow over the course of the semester.

Assignments: (none)

Key Questions:
1. How do you define cybersecurity?
2. What is the most important element in the cybersecurity landscape?
3. How does cybersecurity compare to other national security priorities?

Readings: Snider, Keren, et. al. “Cyber Attacks, Cyber Threats, and Attitudes Towards Cyber Policies.” *Journal of Cybersecurity*. Vol 7, No 1. 2021. 11 pages.
(Instructor will provide .pdf)

Module 2 – September 6 — Cyber Tools and Tactics

Summary: This module explores the diversity of different cyber tools and tactics that adversaries have employed against the United States and other targets.

Assignments: (none)

Key Questions:
1. Why are cyber operations so difficult to detect in advance?
2. What cyber security practices help to minimize the vulnerability or impact of cyber attacks?
3. Of these types of cyber methods—malware, ransomware, doxing, or misinformation operations—which concerns you the most and why?

Readings: Lewis, James and Wood, Georgia. Evolving Cyber Operations and Capabilities. *Center for Strategic and International Studies*. May 2023. 64 pages.
(Instructor will provide .pdf)

Module 3 – September 11 & 13 — Nation State Threats – Russia

Summary: This module examines the cybersecurity challenges posed by Russia and China. It evaluates the different methods and tools Russia has utilized to conduct operations, and how cyber operations fit into its overall national security strategy.

Assignments: Summary memo #1 due 9am, Monday September 11

Key Questions:

1. What makes the Russian cyber threat so significant?
2. What is the relationship between criminal hacking groups and government security services in Russia?
3. How do cyber operations fit within Russia's overall national security agenda?

Readings:

Jensen, Benjamin, et. al. "Fancy Bears and Digital Trolls: Cyber Strategy with a Digital Twist." *Journal of Strategic Studies*. Vol 42, No 2. 2019. 24 pages.
(Instructor will provide .pdf)

"Russia's Strategy in Cyberspace. *NATO Strategic Communications Centre for Excellence*. June 2021. 42. Pages.
(Instructor will provide .pdf)

"Evolution of Russian Cyber Tactics and Operations." *Center for Strategic and International Studies*. 25 March 2021. 50 minutes.
https://www.youtube.com/watch?v=LbZBIP1Ylrk

Module 4 – September 18 & 20 Nation State Threats – China

Summary: This module examines the cybersecurity challenges posed by China. It evaluates the different methods and tools it has utilized to conduct operations, and how cyber operations fit into its overall national security strategy.

Guest speaker: Monday, September 18 - TBD

Assignments: Summary memo #2 due 9am, Monday September 18

Key Questions:

1. What are the differences and similarities between Russian and Chinese cyber operations?
2. How does China use its security services to conduct cyber operations?
3. How do cyber operations fit within China's overall national security agenda?

Readings:

Jiang, Chaoyi. "Decoding China's Perspectives on Cyber Warfare." *Chinese Journal of International Law*. 2021. 56 pages.
(Instructor will provide .pdf)

"Chinese Cyber Espionage Evolves to Support Higher Level Missions." FireEye, Inc. 26 December 2019. (39 minutes) https://www.youtube.com/watch?v=mSk6I6egRD4

Module 5 – September 25 & 27 **Nation State Threats – Iran and North Korea**

Summary: This module examines the cybersecurity challenges posed by Iran and North Korea. It evaluates the different methods and tools these governments have utilized to conduct operations, and how cyber operations fit into their overall national security strategies.

Assignments: Summary memo #3 due 9am, Monday September 25

Key Questions:
1. What are the differences and similarities between Iranian and North Korean cyber operations?
2. How do both governments use their security services to conduct cyber operations?
3. How do cyber operations fit within both governments' overall national security agendas?

Readings: Fixler, Annie. "The Cyber Threat From Iran After the Death of Soleimani." *CTC Sentinel*. Vol 13, No 2. February 2020. 20 pages. https://ctc.usma.edu/cyber-threat-iran-death-soleimani/

North Korea's Cyber Strategy. *Recorded Future*. June 2023. 19 pages. (Instructor will provide .pdf)

"Life Inside North Korea's Hacker Army." *Bloomberg Quick Take*. 23 February 2021. (13 minutes) https://www.youtube.com/watch?v=7A6I-NLzIOI

Module 6 – October 2 & 4 **Non-State Threats: Hackers and Criminal Groups**

Summary: This module examines the cybersecurity challenges posed by foreign-based hackers and criminal groups. It evaluates the different methods and tools these adversaries have used, and the relationships they have with foreign governments on whose soil they operate.

Assignments: Summary memo #4 due 9am, Monday October 2

Key Questions:
1. How are the goals and objectives of hackers and criminal groups different from foreign governments?
2. What tactics and tools do hackers and criminal groups use?
3. What is the relationship between hackers and criminal groups and the foreign governments on whose soil they operate?

Readings: da Cruz, Jose and Pedron, Stephanie. "Cyber Mercenaries: A New Threat to National Security." *International Social Science Review*. Vol 96, Vol 2. 35 pages.
(Instructor will provide .pdf)

"Cybercrime: Understanding the Online Business Model." *UK National Cyber Security Centre*. 12 pages.
(Instructor will provide .pdf)

"The Russian Hackers Being Hunted by the West." *BBC News*. 19 November 2021. (13 minutes)
https://www.youtube.com/watch?v=UG1lJaJsru8

Module 7 – October 9 & 11 US Cybersecurity Policy Frameworks

Summary: This module traces the evolution of U.S. cybersecurity strategy and policy over the last several decades, from the Reagan Administration through the Biden Administration.

Assignments: **Policy memo #1, Wednesday October 11**

Key Questions: 1. What are the biggest changes in US cyber policy since the 1980s?
2. What key events or attacks have influenced the direction of US cybersecurity policy?
3. How does the Biden administration's 2023 strategy compare to others from previous administrations?

Readings: Warner, Michael. "Cybersecurity – A Pre History." *Intelligence and National Security*. Vol 27, No 5. 2012. 19 pages.
(Instructor will provide .pdf)

White House. *National Cybersecurity Strategy*. March 2023. 39 pages.
https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

Module 8 – October 18 Cybersecurity Roles & Responsibilities

Summary: This module examines current US government cybersecurity constructs and organizational responsibilities.

Assignments: (none)

Key Questions:

1. Which US government department or agency do you think has the most important role in cybersecurity?
2. What do you think is the main strength in the current US federal cybersecurity enterprise?   .
3. What do you think is the biggest weakness in the current US federal cybersecurity enterprise?

Readings: (none)

Module 9 – October 23 & 25 Policy Approaches: Military

Summary: This module examines how DoD is currently organized on cyber issues and the laws, rules, and regulations governing the use of cyber operations. It also includes the student policy panel that assesses the pros/cons of the 2023 DoD Cyber Strategy.

Assignments: **Student panel #1, Wednesday October 25 – DoD 2023 Cyber Strategy pros/cons**

Key Questions:

1. How does the Law of Armed Conflict (LOAC) apply in the cyber domain?
2. What are the rules and regulations around DoD's use of cyber operations?
3. How can the United States be more transparent in its conduct of cyberwarfare while still preserving operational security and strategic ambiguity?

Readings:

Department of Defense. 2023 Cyber Strategy. September 2023. 24 pages.
https://media.defense.gov/2023/Sep/12/2003299076/-1/-1/1/2023_DOD_Cyber_Strategy_Summary.PDF

Schneider, Jacquelyn. "A Strategic Cyber No-First Use Policy? Addressing the US Cyber Strategy Problem." *Washington Quarterly*, Vol 43, No 2. 2020. 18 pages.
(Instructor will provide .pdf)

Module 10 – October 30 & November 1 Policy Approaches: Diplomatic

Summary: This module examines how the US Department of State is organized around cybersecurity and the role of cyber ethics and norms in diplomacy.

Assignments: **Student panel #3, Wednesday November 2 – 2021 Cyber Diplomacy Act pros/cons**

Key Questions:

1. What lessons can be drawn from previous arms control treaties?
2. What ethical and legal norms should be considered in cyber diplomacy?
3. What other initiatives should the Department of State pursue in the cyber diplomacy field?

Readings:

Aramitsu, Louise. "A Treaty for Governing Cyber Weapons: Potential Benefits and Practical Limitations." *4th International Conference on Cyber Conflict*. 2012. 19 pages. https://ccdcoe.org/uploads/2012/01/2_3_Arimatsu_ATreatyForGoverningCyber-Weapons.pdf

Schmitt, Michael. "International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed." *Harvard International Law Journal*, Vol. 54. December 2012. 25 pages. https://harvardilj.org/wp-content/uploads/sites/15/2012/12/HILJ-Online_54_Schmitt.pdf

Module 11 – November 6 & 8 Policy Approaches: Homeland Security and Law Enforcement

Summary: This module examines how DHS and FBI are organized around cybersecurity and the different areas of responsibilities within each organization.

Assignments: **Student panel #3, Wednesday November 8 – CISA 2024-2026 Strategic Plan pros/cons**

Key Questions:

1. How have the FBI and DHS evolved their focus on cybersecurity?
2. What challenges do both FBI and DHS face with the sharing of classified intelligence on cyber threats to stakeholders in the United States?
3. What more can DHS do to strengthen its relationship with the private sector when it comes to cyber security defensive measures?

Readings:

"CISA Strategic Plan, 2024-2026." *CISA/DHS*. August 2023. 36 pages. https://www.cisa.gov/sites/default/files/2023-08/FY2024-2026_Cybersecurity_Strategic_Plan.pdf

Vorndran, Bryan. "Oversight of the FBI's Cyber Division." *FBI.gov*. 29 March 2022. 10 pages. https://www.fbi.gov/news/testimony/oversight-of-the-fbi-cyber-division-032922

Module 12 – November 13 & 15 **Policy Approaches: Artificial Intelligence**

Summary: This module explores the impact of artificial intelligence in the US military, intelligence, and law enforcement domains and federal approaches from the White House and Congress to keep up with competitors and adversaries on this front.

Assignments: **Student panel #4, Wednesday November 15 – 2021 Artificial Intelligence Commission Report pros/cons**

Key Questions: 1. What are some of the key artificial intelligence developments in the national security domain?
2. What challenges does the United States face in moving farther along in artificial intelligence?
3. What gains have adversaries and competitors made on the artificial intelligence front, and what lessons can the United States draw?

Readings: "Artificial Intelligence and National Security." *Bipartisan Policy Center*. June 2020. 18 pages. bipartisanpolicy.org/download/?file=/wp-content/uploads/2020/07/BPC-Artificial-Intelligence-and-National-Security_Brief-Final-1.pdf

Burgess, Matt. "The Hacking of ChatGPT is Just Getting Started." *Wired Magazine*. April 1, 2023. 5 pages. https://www.wired.com/story/chatgpt-jailbreak-generative-ai-hacking/

National Security Commission on Artificial Intelligence Final Report – Executive Summary. March 2021. 10 pages. https://www.nscai.gov/wp-content/uploads/2021/03/Final_Report_Executive_Summary.pdf

Module 13 – November 20 **Guest Speaker**

Summary: Heading into the Thanksgiving break, this module will involve a guest speaker who can discuss one of the threat or policy-related cybersecurity topics covered in the course up until this point.

Guest speaker: Barbara McQuade, Professor from Practice, University of Michigan School of Law and former US Attorney for the Eastern District of Michigan
https://michigan.law.umich.edu/faculty-and-scholarship/our-faculty/barbara-l-mcquade

Assignments: (none)

Readings: (none)

***No class 22 November - Thanksgiving Break**

Module 14 – November 27 & 29 Policy Approaches: Information-Sharing

Summary: This module explores how the US government has attempted to facilitate the sharing of cyber threat-related information with the private sector, and likewise the encourage private sector companies to reciprocate despite reservations and hesitations for doing so.

Assignments: **Student panel #5, Wednesday November 29 – Cyber Incident Reporting for Critical Infrastructure Act of 2022 pros/cons**

Key Questions: 1. What difficulties do private sector companies face with respect to information-sharing on cyber threats and response measures?
2. What are some of the biggest challenges for the federal government with respect to sharing classified intelligence or sensitive information with different stakeholders?
3. What lessons can be drawn from the counterterrorism world with respect to the top-down and bottom-up mechanisms for information-sharing on cyber threats?

Readings: Bakis, Bruce and Wang, Edward. "Building a National Cyber Information-Sharing Ecosystem: Chapters 1-3." *MITRE Corporation*. May 2017. 50 pages.
(Instructor will provide .pdf)

Turetsky, David, et. al. "Success Stories in Cyber Information-Sharing." *University of Albany*. 20 July 2020. 15 pages.
(Instructor will provide .pdf)

Module 15 – December 4 & 6 Policy Approaches: Election Security

Summary: This module explores different approaches, standards, and laws that state and local governments have adopted in response to cyber threats, and uses the election security issue to highlight strengths and weaknesses on the cybersecurity front.

Assignments: **Policy Memo #2, Wednesday December 6; Student panel #6 due Wednesday December 6 – HR 2722, the SAFE Act pros/cons**

Key Questions: 1. What is the difference between election influence and election interference?

2. What aspect of voting in the United States is more vulnerable to cyber-enabled methods—electronic voting or perceptions of political candidates?

3. What additional measures should state and local governments adopt when it comes to election security?

Readings:

Cortes, Edgar, et. al. “Beyond 2020: Policy Recommendations for the Future of Election Security.” *Brennan Center for Justice*. February 2021. 40 pages.
(Instructor will provide .pdf)

Manpearl, Eric. “Securing U.S. Election Systems: Designating U.S. Election Systems as Critical Infrastructure and Instituting Election Security Reforms.” *Boston University Journal of Science and Technology Law*, Vol 24, No 1. 2018. 28 pages.
(Instructor will provide .pdf)