Syllabus – Law 416 – Cybersecurity Law Seminar

Antonin Scalia Law School at George Mason University – Fall 2025

Profs. Shannon Togawa Mercer & Jamil N. Jaffer

Brief Course Description:

This seminar course will provide students exposure to the key legal and policy issues related to cybersecurity, including the legal authorities and obligations of both the government and the private sector with respect to protecting computer systems and networks, as well as the national security aspects of the cyber domain including authorities related to offensive activities in cyberspace. The course will include a survey of federal laws, executive orders, regulations, and cases related to surveillance, cyber intrusions by private and nation-state actors, data breaches, and privacy and civil liberties matters, among other things. The course will also explore the legislative and technology landscape in this dynamic area and will provide students with opportunities to discuss cutting-edge issues at the intersection of law, technology, and policy.

Learning Outcomes:

By the end of the course students should have acquired/be able to:

1. Understand the different types of cybersecurity threats posed to computer systems and networks.

2. Identify national security implications from threats in the cyber domain.

3. Apply the legal authorities and obligations of government and the private sector to protect computer systems and networks.

4. Critically analyze the national security policy decisions, directives, and actions for developing and implementing cybersecurity policy in relation to federal laws, executive orders, regulations, and ongoing cases.

Class Format:

- Seminar of 10-20 students; two credits; one two-hour **in-person** class per week.
- **Active participation in class discussions is required, and students are expected to be fully prepared** for each class session.

Class Details:

- Thursdays – 8:10 PM – 10:10 PM ET

Grading:

- Grades will be based on a 20-25 page paper on cybersecurity law and class participation consistent with the law school grading policy.
- Class attendance will be taken consistent with the law school policy.

Paper Due Date:

- **Friday, December 5, 2025 – 11:00 pm ET**
  - Papers are due via email to both professors by no later than the date and time above.
  - **Late papers will receive a full grade deduction for every day the paper is late** based on current law school policy.

Office Hours:

- By appointment only; contact **nsisched@gmu.edu** to coordinate meetings.

Faculty Contact Information:

- **Professor Shannon Togawa Mercer**: smercer4@gmu.edu
- **Professor Jamil N. Jaffer**: jjaffer@gmu.edu

Course Specific Policies:

- Students are expected to attend and participate in every class.
- Students are expected to complete the assigned readings before each week's class and to come prepared to discuss them.
- Socratic dialogues will be employed by the instructors to facilitate learning outcomes.
- If unforeseen circumstances prevent a student from preparing for class, the student is nonetheless encouraged to attend and should inform the instructors in advance if they are not prepared to be called upon.
- All students are expected to treat each other and the instructors with courtesy and respect.
- Ideas and theories are welcome and encouraged to be challenged, but such critiques should never take the form of personal attacks on another speaker within the classroom setting.
- The instructors seek a safe academic environment wherein ethical and philosophical issues can be intellectually explored.

- Students must use their GMU email account to receive important University information, including communications related to this class.

- The instructors will not respond to messages sent from or send messages to a non-Mason email address. it is always best to text the instructors and cc: the nsisched@gmu.edu email address in addition to sending emails to ensure prompt responses.

Use of Generative AI:

- Pursuant to Academic Regulation 4-3(b), the instructor of this course expressly permits the use of generative artificial intelligence (GAI) (as defined in Academic Regulation 4-3(a)) as an appropriate resource for work in this this course, including to prepare for class and to prepare the exam in this class, so long as students using GAI strictly comply with the requirements provided herein.
- Pursuant to Academic Regulation 4-3(e), in order to permissibly use GAI in this course, if students prepare any written work for use during the course or if GAI is used to prepare for oral presentations during their panel week, students using GAI must:
    - (1) disclose, in the first footnote of any written work submitted for the course, whether for a grade or not, whether they have used GAI in any manner in the course of drafting or writing of such written work and the specific GAI source(s) used in the paper and, if GAI has been used, certify that they have reviewed and are in strict compliance with the policies set forth in the Academic Regulations and herein, as follows:
        - "I, [insert student name], certify that I have reviewed Scalia Law Academic Regulation(s) related to the use of generative artificial intelligence (GAI) and the provisions and policies set forth in the syllabus for this course. Pursuant to those regulations, provisions, and policies, I disclose that I have used GAI in the course of drafting or writing of this written work, and specifically that I have used the following GAI source(s): [insert GAI source name(s)]. I hereby certify that I am in strict compliance with the policies set forth in the Academic Regulations and the syllabus for this course."
    - (2) disclose verbally in any oral presentation that relies on generative AI that they have used such sources and note the specific GAI source(s) used;
    - (3) obtain the sources underlying any GAI generated output and independently verify any claims made therein;
    - (4) not use any GAI generated output where the student cannot obtain the sources underlying the GAI generated output and independently verify any claims made therein;
    - (5) not use any GAI generated output in any form for written work or oral presentations whether such output is used verbatim, paraphrased, or otherwise used (including to generate independent work or analysis), unless such output work is properly quoted and/or cited in written form or described verbally in an oral presentation, just as one would with any standard written text;

  - (6) in written work, provide citations to GAI generated output that cite both the GAI generating source(s) as well as the underlying source from where the material originated and the sources used to verify the claims made.

- Pursuant to Academic Regulation 4-3(f), students who use GAI in an manner inconsistent with the Academic Regulations and this syllabus and the policies provided therein, may be subject to the disciplinary sanctions set forth in Section 3.01 of the Honor Code, as the use of GAI not in compliance with such provisions and policies in written work is considered academic dishonestly involving cheating in violation of Section 1.01.1 and/or 1.01.5 of the Honor Code.

- Law School instructors and administrators, including those for this course, reserve the right to use AI detection software to find instances of GAI in student written work.

Class Recordings Prohibited:

- Pursuant to Academic Regulation 4-2.2, no portion of a class session or an examination may be preserved by means of a recording device such as an audio recording device, camera, or computer.
- Any exceptions to this policy must be expressly authorized in writing by the instructor(s).
- The instructors do not intend to record the weekly course meetings.

Course Materials:

- All course materials are available via the Internet (as linked below), via TWEN (if specifically noted below) or, if caselaw, statutes or secondary legal materials including law review articles, on Westlaw or Lexis-Nexis.
- ** Given the developing nature of this area of law, it is likely that the syllabus and readings will be updated over the course of the semester; therefore, **please regularly check your email for updates to the syllabus and assignments / readings**. **

Course Assignments:

Week 1: Introduction to Computer Networks and Cyber Threats

1. Congressional Research Service, Cybersecurity: A Primer (Jan. 8, 2025) – pp. 1-2 (Link)
2. Robert M. Chesney, CHESNEY ON CYBERSECURITY LAW, POLICY, AND INSTITUTIONS (v. 3.1) – Introduction to Key Terms & Concepts – pp. 11-16 (hereinafter "Chesney on Cybersecurity") (Link)
3. Office of the Director of National Intelligence, Annual Threat Assessment (March 2025) – China-cyber p. 11-13; Russia-cyber p. 19 (Link)
4. Executive Office of the President, Sustaining Select Efforts to Strengthen the Nation's Cybersecurity and Amending Executive Order 13694 and Executive Order 14144 Fact Sheet (June 6, 2025) (Link)

Week 2: Nation-State Hacking, Political Manipulation, and Federal Law

1. Chesney on Cybersecurity – *What if the Attacker is a Foreign Government (I-IV)* – pp. 43-65 (Link) (***note: there is no need to read the internally referenced articles unless they are of interest to you***).
2. Chesney on Cybersecurity – *Holiday Bear and SolarWinds* – pp. 3-9 (Link)
3. Brian Barrett, SolarWinds Hack is Historic Mess, Wired (Dec. 19, 2020) – pp. 1-3 (Link)
4. Congressional Research Service, *Salt Typhoon* Hacks of Telecommunications Companies and Federal Response Implications (Jan. 23, 2025) – pp. 1-2 (Link)
5. Microsoft Digital Defense Report 2024 –Report – pp. 12-26 (Link)

Week 3: Hacking, Ransomware, and the Computer Fraud & Abuse Act

1. Chesney on Cybersecurity – *Computer Fraud & Abuse Act* – pp. 19-21 (Link)
2. *U.S. v. Morris*, 928 F.2d 504, 504-11 (2d Cir. 1991) (Westlaw/LEXIS)
3. Congressional Research Service, *Cybercrime and the Law: Primer on the Computer Fraud and Abuse Act and Related Statutes – Challenges in Prosecuting Cybercrimes Originating Abroad* – pp. 38 - 40 (May 16, 2023) (Link).
4. David Sanger & Nicole Perlroth, *Pipeline Attack Yields Urgent Lessons About U.S. Cybersecurity*, New York Times (May 14, 2021) – pp. 1-3 (Link)
5. Reuters, *UnitedHealth says hack at tech unit impacted 190 million people* (Jan. 24, 2025) (Link)
6. Zach Montague, *Russian Ransomware Group Breached Federal Agencies in Cyberattack*, New York Times (June 15, 2023) (Link)
7. Tom Uren, Four Key Players Drive Scattered Spider (read until "Intelligence for Sale Will Annoy Beijing but Amuse Us Immensely"), Lawfare (July 11, 2025) (Link)

Week 4: Economics of Cyber Threats

1. Chesney on Cybersecurity – *Private Lawsuits* – pp. 84-94 (Link)
2. Ross Anderson, *Why Information Security Is Hard – An Economic Perspective* (2001) – pp.1-7 (Link)
3. IBM Security X-Force, Cost of a Data Breach 2024 – Factors that decreased or increased the average breach cost – pp. 22-27 (TWEN)
4. Estefania Vergara Cobos and Selcen Cakir, A Review of the Economic Costs of Cyber Incident (2024) World Bank – pp. 2- 13 (Link)
5. Lauren Feiner, CrowdStrike CEO to testify about massive outage that halted flights and hospitals, The Verge (July 22, 2024) (Link)
6. Sriparna Roy & Leroy Leo, UnitedHealth to take up to $1.6 billion hit this year from Change hack, Reuters (April 16, 2024) (Link)

Week 5: Private Hacking Enforcement and Cybersecurity Regulation:

1. Chesney on Cybersecurity – *Civil Liability Under the CFAA* – pp. 30-42 (Link)
2. Chesney on Cybersecurity – *The Role of Regulators* – pp. 67-70 (Link)
3. Chesney on Cybersecurity – *Private Lawsuits* – pp. 95-103 (Link)
4. *FTC v. Wyndham Worldwide,* 799 F.3d 236, 240-258 (3rd Cir. 2015) (Westlaw/LEXIS)
5. Mike Scarcella & David Shepardson, *AT&T's $177-million data breach settlement wins US court approval*, Reuters (June 20, 2025)(Link)

6. FTC, *FTC Finalizes Order with GoDaddy over Data Security Failures* (May 21, 2025) (Link)
7. Arianna Evers, Shervin Taheran, Shannon Togawa Mercer, 8 Questions to Ask Before Final CISA Breach Reporting Rule, Law360 (May 8, 2024) – p 1. (Link)

Week 6: Electronic Surveillance

1. *Katz v. United States*, 389 US 347 (1967) (Westlaw/LEXIS)
2. *Smith v. Maryland*, 442 U.S. 735 (1979) (Westlaw/LEXIS)
3. *Carpenter v. United States*, 138 S. Ct. 2206 (2018) (Westlaw/LEXIS)

Week 7: AI and Cybersecurity

1. Microsoft Digital Defense Report 2024 (AI's impact on cybersecurity) –pp. 84-100 (Link)
2. Secure, Empower, Advance: How AI Can Reverse the Defender's Dilemma, Google (Feb. 2024) – pp. 2-5, 16-21, 31-37
3. NY Department of Financial Services, Industry Letter, (Oct. 16, 2024) (Link)
4. Dave Aitel, Dan Geer, *AI and Secure Code Generation*, Lawfare (June 27, 2025)
5. Ben Nimmo, Albert Zhang, Matthew Richard, Nathaniel Hartley, *Disrupting malicious uses of our models: an update February 2025*, OpenAI (February 2025) – pp. 10 – 13, 27 – 28 (Link)
6. Deploying AI Systems Securely: Best Practices for Deploying Secure and Resilient AI Systems, Cybersecurity and Infrastructure Security Agency (Apr. 2024) – pp. 1-10

Week 8: Foreign Intelligence

1. *ACLU v. Clapper*, 785 F.3d 787 (2d Cir. 2015) (Westlaw/LEXIS)
2. *United States v. Hasbajrami*, 945 F.3d 641 (2d Cir. 2019) (Westlaw/LEXIS)
3. Privacy and Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702*, Executive Summary – pp. 1-7 (Sept 28, 2023) (Link) **(Note: If printing out, please only print the pages you're reading; file is very long)**
4. Congressional Research Service, *FISA Section 702 Sunset, Authorization, and Potential Extension*, (April 17, 2024) – pp. 1-4

Week 9: Cybersecurity and the Fourth Amendment

1. *In re: Yahoo Mail Litigation*, 7 F.Supp.3d 1016 (N.D. Cal. 2014) (Westlaw/LEXIS)
2. Congressional Research Service, Geofence Warrants and the Fourth Amendment (May 9, 2025) – pp. 1-6 (Link)
3. Podcast: Lawfare Daily: Orin Kerr on the Digital Fourth Amendment (Jan. 9, 2025) (*transcript included on webpage*)

Note: Preliminary Paper Topics Due [*voluntary*]

Week 10: Privacy and Encryption

1. Congressional Research Service, *Data Protection and Privacy Law: An Introduction* (May 2022) – pp. 1-2 (Link)
2. Congressional Research Service, *Data Protection Law: An Overview* (Mar. 2019) – pp. 1- 7, 25-40 (Link)

3. Congressional Research Service, *EU Data Protection Rules and US Implications* (July 2020) – pp. 1-2 (Link)
4. Congressional Research Service, *Law Enforcement and Technology: The "Lawful Access" Debate* (Jan 2025) – pp. 1-2 (Link)
5. *In Re: Grand Jury Subpoena*, 670 F.3d 1335 (11th Cir. 2012) (Westlaw/LEXIS)

NOTE: FINAL PAPER TOPICS DUE THIS WEEK

Week 11: Protecting the Private Sector: Information Sharing & Collective Defense

1. Chesney on Cybersecurity – *Facilitating Information Sharing to Better Protect the Private Sector* – pp. 114-116, 121-132 (Link)
2. Congressional Research Service, *The Cybersecurity Information Sharing Act of 2015: Expiring Provisions*, (April 2025) – pp. 1-2 (Link)
3. Keith B. Alexander, et. al., *Clear Thinking About Protecting the Nation in the Cyber Domain*, Cyber Defense Review (Mar. 2017) – pp. 29-36 (TWEN)
4. Cyber National Mission Force Public Affairs, CYBERCOM's "Under Advisement" to increase private sector partnerships, industry data-sharing in 2023 (June 29, 2023) (Link)

Week 12: Offensive Cyber Activities: International Law and Deterrence

1. Eric Talbot Jensen, *The Tallinn Manual 2.0: Highlights and Insights*, Georgetown Journal of International Law (2017) – pp. 736-757, 772-778 (Link)
2. Jack Goldsmith, *Cybersecurity Treaties: A Skeptical View* (Feb. 2011) – pp. 1-16 (Link)
3. Keith B. Alexander & Jamil N. Jaffer, *Only a Serious Response Will Reverse Iran's Growing Aggression* (Oct. 2019) – pp. 1-3 (Link)
4. Davey Winder, Paris Olympics Security Warning – Russian Hackers Threaten 2024 Games, Forbes (July 19, 2024) (Link)
5. Martin Matishak, 22 'hunt forward' missions deployed overseas in 2023, Cyber Command leader says, The Record (April 10, 2024) (Link)

Week 13: Offensive Cyber Activities: Domestic Law and Deterrence

1. Congressional Research Service, Defense Primer: Cyberspace Operations (Nov. 29, 2024) – pp. 1-2 (Link)
2. Senate Armed Services Committee FY 26 NDAA – pp. 9 - 11
3. Department of Defense (DOD) Cyber Strategy – 2023 – Summary, pp. 1-8 (Link)
4. Robert Chesney, *Hackback is Back: Assessing the Active Cyber Defense Certainty Act*, Lawfare (June 14, 2019)
5. U.S. Cyber Command Public Affairs, Commander, U.S. Cyber Command rolls out new Strategic Priorities (May 18, 2023)(Link)

Optional Reading:

- Week 2: Sara Weidemar, NATO and Article 5 in Cyberspace (May 2023) pp. 1-4 (Link)
- Week 3: *Van Buren v. United States*, 141 S. Ct. 1648, 1651-69 (2021) (Westlaw/LEXIS)
- Week6: *United States v. Jones*, 565 U.S. 400 (2012) (Westlaw/LEXIS); *Riley v. California*, 134 S. Ct. 2473 (2014) (Westlaw/LEXIS); **An outside perspective on US surveillance and privacy:** Andrew Serwin, An Overview of US Surveillance in Light of 'Schrems II', IAPP White Paper (August 2020) – pp. 1- 31 (Link)