ANTONIN SCALIA LAW SCHOOL
George Mason University

FALL 2026 COURSE SYLLABUS

Course Number: 416-001

Course Title: Cybersecurity Law Seminar

Credit Hours: 2

Grading Mode: Letter grade

Meeting Day(s)/ Time(s): THUR. 9:40a-11:40a

Meeting Mode: In-person

Exam Day(s)/ Time(s): N/A

Final Exam Mode: PAPER

Prerequisite(s): N/A

Corequisite(s): N/A

Instructor(s): Bishop Garrison

Contact Information: bgarris@gmu.edu

Office Hours:

- By appointment only.
- Students may contact the instructors in class or via phone or email to set up a time to speak outside of class.

Course Overview

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.

Course 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.

Reading(s) & Supplement(s):

All course materials are cases or articles available on Westlaw or Lexis-Nexis or posted on TWEN. Materials posted on TWEN are indicated below.

** 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 and TWEN for updates to the syllabus and readings**. **

Grading Policies

Grades will be based on a 20-25 page paper on cybersecurity law and class participation

Participation & Preparation:

- Active participation in class discussions is required and students are expected to be fully prepared for each class session. We will also be taking class attendance, consistent with the law school policy.

Final Paper Due Date:

- **Friday, October 29, 2026 – 11:59 pm ET (WEEK 11)**
    - Paper are due via email to both professors by no later than the date and time above.
    - ** Please note that **late papers will receive a full grade deduction for**

every day the paper is late based on current law school policy, so please turn papers in on time. **

- Voluntary "Preliminary" Paper Outline: if you wish to get feedback from Prof. Garrison on your proposed paper topic and/or paper structure, you may do so no later than Week 9. Professor Garrison will discuss this option further in class.

Additional Information:

- 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 MasonLive 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.

Classroom Policies

Attendance: Per AR 3-1.4, “maintenance of matriculation requires regular class preparation, participation and attendance, registration in the course of study required for the student’s program (full-time or part-time), successive registration for each fall and spring term of each academic year until study is completed, and compliance with all other relevant requirements.”

Absences: Per AR 4-1.1, “if a student is absent for any reason for more than 20 percent of the sessions of a course, the student is not eligible for credit in that course. A student who is not present for at least 75 percent of a session of the course is absent from that session.”

Use of Technology & AI:

Strict Use Policy: The use of generative AI tools is not permitted for any coursework in this course. Unauthorized use will be treated as a violation of academic standards.

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 <u>not</u> intend to record the weekly course meetings.

Course Schedule & Assignments

Week 1: Introduction to Computer Networks and Cyber Threats (August 20, 2026)

1. Congressional Research Service, Cybersecurity: A Primer (Dec. 15, 2020) – pp. 1-2 (TWEN or use link)
2. Robert M. Chesney, CHESNEY ON CYBERSECURITY LAW, POLICY, AND INSTITUTIONS (v. 2.1) – Introduction to Key Terms & Concepts – pp. 11-16 (hereinafter "Chesney on Cybersecurity") (TWEN or use link)
3. U.S. National Cyber Strategy 2026
4. Office of the Director of National Intelligence, Annual Threat Assessment of the U.S. Intelligence Community (2025) – Major State Actors pp. 9-30 (Overview and Cyber section for each country)

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

1. Chesney on Cybersecurity – *Holiday Bear and SolarWinds* – pp. 3-9 (TWEN or use link)
2. Brian Barrett, SolarWinds Hack is Historic Mess, Wired (Dec. 19, 2020) – pp. 1-3 (TWEN or use link)
3. Chesney on Cybersecurity – *Holiday Bear and SolarWinds* – pp. 43-66 (TWEN or use link) (note: there is no need to read the internally referenced articles unless they are of interest to you).
4. Congressional Research Service, *The Designation of Election Systems as Critical Infrastructure* (Sept. 2019) – pp. 1-2 (TWEN or use link)
5. Microsoft Digital Defense Report 2023 –Report: pp. 46-70 (TWEN)
6. CISA, Nation-State Threats, Overview (2026 update):

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

1. David Sanger, Clifford Krause, & Nicole Perlroth, *Cyberattack Forces a Shutdown of a Top U.S. Pipeline*, New York Times (May 8, 2021) – pp. 1-4 (TWEN or use link)
2. David Sanger & Nicole Perlroth, *Pipeline Attack Yields Urgent Lessons About U.S. Cybersecurity*, New York Times (May 14, 2021) – pp. 1-3 (TWEN or use link)
3. Chesney on Cybersecurity – *Computer Fraud & Abuse Act* – pp. 17-21 (TWEN or use link)
4. *U.S. v. Morris*, 928 F.2d 504, 504-11 (2d Cir. 1991) (Westlaw/LEXIS)
5. *Van Buren v. United States*, 141 S. Ct. 1648, 1651-69 (2021) (Westlaw/LEXIS)
6. Zach Montague, *Russian Ransomware Group Breached Federal Agencies*

in Cyberattack, New York Times (June 15, 2023)

Week 4: Economics of Cyber Threats

1. The White House, *Heartbleed: Understanding Why We Disclose Cyber Vulnerabilities* (Apr. 28, 2014) – pp. 1-2 (TWEN or use link)
2. Ross Anderson, *Why Information Security Is Hard – An Economic Perspective* (2001) – pp. 1-7 (TWEN or use link)
3. Chesney on Cybersecurity – *Private Lawsuits* – pp. 84-94 (TWEN or use link)
4. World Economic Forum Annual Meeting on Cybersecurity 2026, The Rise of Cybersecurity as an Economic Strategy,
5. Robert Hart, Tech Giants Make 'Voluntary' Pledge to Develop Responsible AI – Including OpenAI and Google – White House Says, Forbes (July 21, 2023)
6. The New Economics of Cyber Risk (Deloitte WSJ Op-Ed, May 26, 2026),
7. Lauren Feiner, CrowdStrike CEO to testify about massive outage that halted flights and hospitals, The Verge (July 22, 2024)

Week 5: Private Hacking Enforcement and Cybersecurity Regulation:

1. Chesney on Cybersecurity – *Civil Liability Under the CFAA* – pp. 30-42 (TWEN or use link)
2. Chesney on Cybersecurity – *The Role of Regulators* – pp. 67-70 (TWEN or use link)
3. *FTC v. Wyndham Worldwide,* 799 F.3d 236, 240-258 (3rd Cir. 2015) (Westlaw/LEXIS)
4. *LabMD, Inc. v. Federal Trade Commission,* 894 F.3d 1221, 1223-38 (11th Cir. 2018) (Westlaw/LEXIS)
5. Chesney on Cybersecurity – *Private Lawsuits* – pp. 95-103 (TWEN or use link)
6. Executive Office of the President, *National Cybersecurity Strategy* (March 2023) – pp. 23-28 (Pillar 4)

Week 6: Electronic Surveillance: Background Legal Principles

1. *Katz v. United States*, 389 US 347 (1967) (Westlaw/LEXIS)
2. *Smith v. Maryland*, 442 U.S. 735 (1979) (Westlaw/LEXIS)
3. *United States v. McLaren*, 957 F. Supp. 215 (M.D. Fla. 1997) (Westlaw/LEXIS)
4. *United States v. Warshak*, 631 F.3d 266, 282-290 (6th Cir. 2010) (Westlaw/LEXIS)
5. Paul Rosenzweig, *The Evolution of Wiretapping*, Engage – pp. 83-87 (Sept. 2011) (TWEN)

Week 7: Electronic Surveillance & Technological Advances

1. *In re: Google Street View Electronic Communications Litigation*, 794

F.Supp.2d 1067 (N.D. Cal. 2011) (Westlaw/LEXIS)
2. *United States v. Jones*, 565 U.S. 400 (2012)
3. *Riley v. California*, 134 S. Ct. 2473 (2014)
4. *Carpenter v. United States*, 138 S. Ct. 2206 (2018)

Week 8: Metadata and Foreign Intelligence

1. *ACLU v. Clapper*, 785 F.3d 787 (2d Cir. 2015) (Westlaw/LEXIS)
2. Privacy and Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702*, Executive Summary – pp. 5-15 (July 2014) (TWEN or use link) **(Note: If printing out, please only print pp. 10-20 of the PDF; file is very long)**
3. *In re: Directives*, 551 F.3d 1004 (FISA Ct. Rev. 2008)

(Westlaw/LEXIS)

Week 9: Cybersecurity and the Fourth Amendment

NOTE: FINAL PAPER TOPICS DUE THIS WEEK (OPTIONAL)

1. DOJ Office of Legal Counsel, *Legal Issues relating to the Testing, Use and Deployment of an Intrusion Detection System (Einstein 2.0) to Protect Unclassified Computer Networks in the Executive Branch* (Jan. 9, 2009) – pp. 1-35 (TWEN)
2. DOJ Office of Legal Counsel, *Legality of Intrusion-Detection System to Protect Unclassified Computer Networks in the Executive Branch* (August 2009) – pp. 1-6 (TWEN)
3. *In re: Yahoo Mail Litigation*, 7 F.Supp.3d 1016 (N.D. Cal. 2014)

(Westlaw/LEXIS)

Week 10: Privacy and Encryption

1. Congressional Research Service, *Data Protection and Privacy Law: An Introduction* (May 2019) – pp. 1-2 (TWEN)
2. Congressional Research Service, *Data Protection Law: An Overview* (Mar. 2019) – pp. 1- 7, 25-40 (TWEN)
3. Congressional Research Service, *EU Data Protection Rules and US Implications* (Aug. 2018) – pp. 1-2 (TWEN)
4. Congressional Research Service, *Watching the Watchers: A Comparison of Privacy Bills in the 116th Congress* (Apr. 3, 2020) – pp. 1-5 (TWEN or use link)
5. *In Re: Grand Jury Subpoena*, 670 F.3d 1335 (11th Cir. 2012) (Westlaw/LEXIS)
6. Department of Justice, *Government's Ex Parte Application for an Order Compelling Apple, Inc. to Assist Agents in Search: Memorandum of Points and Authorities* (Feb. 16, 2016) – pp. 3-20 (TWEN)

7. Jamil N. Jaffer & Daniel J. Rosenthal, *Why Apple's Stand Against the F.B.I. Hurts Its Own Customers*, New York Times (Apr. 8, 2016) – pp. 1-3 (TWEN)

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

NOTE: PAPER IS DUE BY FRIDAY 11:59 PM - EMAIL INBOX

1. Chesney on Cybersecurity – *Facilitating Information Sharing to Better Protect the Private Sector* – pp. 114-116, 121-132 (TWEN or use link)
2. CNBC, The Controversial "Surveillance" Act Obama Just Signed (Dec. 22, 2015) (TWEN)
3. Executive Order 14028, *Improving the Nation's Cybersecurity* (May 12, 2021) – pp. 1-3,
   5-7, 8-9, 11-12 (TWEN)
4. Keith B. Alexander, et. al., *Clear Thinking About Protecting the Nation in the Cyber Domain*, Cyber Defense Review (Mar. 2017) – pp. 29-36 (TWEN)

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
2. Jack Goldsmith, *Cybersecurity Treaties: A Skeptical View* (Feb. 2011) – pp. 1-16 (TWEN)
3. Keith B. Alexander & Jamil N. Jaffer, *Only a Serious Response Will Reverse Iran's Growing Aggression* (Oct. 2019) – pp. 1-3 (TWEN)
4. Davey Winder, Paris Olympics Security Warning – Russian Hackers Threaten 2024 Games, Forbes (July 19, 2024)
5. Martin Matishak, 22 'hunt forward' missions deployed overseas in 2023, Cyber Command leader says, The Record (April 10, 2024)

Week 13: Offensive Cyber Activities: Domestic Law and Deterrence

1. Congressional Research Service, Defense Primer: Cyberspace Operations (Dec. 2018) – pp. 1-2 (TWEN)
2. 10 U.S.C. 391-396 – Cyber Matters, pp. 1-12 (TWEN)
3. Department of Defense (DOD) Cyber Strategy – 2023 – Summary, pp. 1-7 (TWEN)
4. Command Vision for U.S. Cyber Command – 2018, pp. 2-10 (TWEN)
5. Keith B. Alexander & Jamil N. Jaffer, *Iranian Cyberattacks Are Coming, Security Experts Warn* (Jan. 2020) – pp. 1-4 (TWEN)

Student Resources

Antonin Scalia Law School Academic Regulations

GMU Common Course Policies Addendum

Mason Square Services

Mason Square Police
Van Metre Hall, Room 110
Emergency - Dial 911
Escort Services - 703-993-8070
Dispatch – 703-993-2810

Student Support and Advocacy Center (SSAC)

Mason Square Sexual Assault Services:
Van Metre Hall, Room 222D
703-993-8186

Notice of Mandatory Reporting of Sexual Assault, Sexual Harassment, Interpersonal Violence, and Stalking:

As a faculty member, I am designated as a "Non-Confidential Employee," and must report all disclosures of sexual assault, sexual harassment, interpersonal violence, and stalking to Mason's Title IX Coordinator per University Policy 1202. If a student wishes to speak with someone confidentially, please contact one of Mason's confidential resources, such as Student Support and Advocacy Center (SSAC) at 703-380-1434 or Counseling and Psychological Services (CAPS) at 703-993-2380. Students may also seek assistance or support measures from Mason's Title IX Coordinator by calling 703-993-8730, or emailing titleix@gmu.edu.

Mason Square Clinic
Van Metre Hall, Room B102
703-993-2831

Counseling and Psychological Services

Student Health Services

Student Disability Services

University Life