INST771 – Foundations of Cybersecurity – Fall 2024

Course Title: Foundations of Cybersecurity
Course Number: INST771
Term: *Fall/2024*
Credits: 3
Course Dates: Aug 27, 2024 – Dec 3, 2024
Course Times: Tuesdays 2:15pm-4:15pm

Professor: Ido Sivan-Sevilla
Pronouns: he/him/his
Office Phone: 301-405-3600
Email: sevilla@umd.edu
Office Hours: Fridays 1pm-2pm via Zoom – should be scheduled via email prior to that Friday every week
Classroom: EDU 3236

Course Description

The rapid and widespread growth in computation, connectivity, and digital storage capacities created a new human-made domain – cyberspace. The cyberspace domain challenges traditional assumptions, boundaries, and opportunities for social life. Most notably, cyberspace changes the meaning, methods, and trust assumptions necessary to achieve security and protect our privacy. Cybersecurity, then, is not merely 'security in cyberspace.' It is the study of how and why the human transition to cyberspace changes security risk assumptions and how to respond to those challenges. The purpose of this class is to provide the fundamentals for understanding the core technical and social components that construct the cybersecurity problem. We will unpack the concepts of vulnerabilities & exploits; discuss their manifestation in different operating systems, supply chain providers, and computer networks; learn how to measure the severity of vulnerabilities; detail the hacking process and corresponding threat intelligence; learn about main threats in the threat landscape; and discuss how and why cybersecurity is governed across top-down & bottom-up governance arrangements.

We will start with understanding what is unique about cyberspace [module #1], explain what is at the core of technical cyber insecurity: exploits and vulnerabilities across mobile, desktops, servers, networks, and third-party software [module #2], overview of the hacking process and corresponding threat intelligence [module #3], survey the threat landscape from nations, criminals, and hacktivists [module #4], and explain what is currently being done for governing the cybersecurity problem across top-down and bottom-up governance mechanisms [module #5].

By the end of this class, students will have a comprehensive understanding of the cybersecurity problem, its history, core components, technical solutions, threat intelligence, and up-to-date governance mechanisms.

No technical background is required to succeed in this class!

Learning Outcomes

After successfully completing this course, you will be able to:

- Articulate how the cyber security field developed from a sociotechnical point of view and what are the incentives structures in place.

- Demonstrate an understanding of the technical structures and protocols of modern telecommunications and existing digital devices that enable cyber insecurity.
- Describe security and legal questions that countries struggle to solve with respect to cybersecurity including abuse of networks and resources and violations of privacy.
- Articulate the hacking process including conducting reconnaissance, exploiting vulnerabilities, establishing presence, and maintaining command and control.
- Categorize threat actors and explore the myriad of the cybersecurity threat landscape including motivations, tactics and tradecraft used by individuals and organizations.
- Explain technologies of governance for cybersecurity. Describe the effects, including direct and indirect, of given security policies or decisions made by corporations, states, and non-profit actors.

Required Resources

There is no required textbook for this course. On ELMS (elms.umd.edu) you will find the course syllabus and schedule, presentation materials, announcements, assignment details, grading rubrics, and assigned readings. Please read the required readings before the date for which they are listed.

Getting the most out of the assigned readings is key for understanding and engaging in class discussion every week. Your reflection on the readings is **25%** of your grade! I expect them to be rich, critical, and when possible, engaging with posts from other students and content from previous classes. Please do not hesitate to ask questions and challenge our current knowledge about the weekly topics.

Course Structure

We will meet in-person, on a weekly basis, to discuss readings and engage with students' points of view, based on your posts in ELMS. It is very (very) important that you read the assigned readings. They were carefully assigned to you, based on their depth and their overall contribution to our course goals. They are not super-intimidating, do not require technical background, but still, very refreshing and revealing when it comes to understanding the foundations of cybersecurity.

Activities, Learning Assessments, and Expectations from Students

Very important: Please make sure you are receiving emails and know how to submit your assignments via ELMS. If it is not the case, please let me know as soon as possible. All our communication and assignment submission will take place via ELMS so you need to make sure you are on top of it.

Learning Assessments	Points Each	Date due
Class Participation & Reading Responses	**25**	Throughout the semester
Vulnerabilities & Exploits Report *[Module #2 Summary]*	**25**	Oct 8th [week #7]
Hacking & Threat Intelligence Analysis *[Module #3 & #4 Summary]*	**25**	Nov 5th [week #11]

Cybersecurity Governance Report *[Module #5 Summary]*	**25**	Dec 3rd [week #15]

Class participation & Reading Responses: The structure of the class is discussion-focused. I will lead the discussion, but I expect all to actively participate. We are a relatively small class, and I am hoping to hear from everyone, every week. This means you are required to finish all assigned readings before each class session and submit your posting by Monday 12pm of every week, allowing me to build on your responses as I prepare the class – please don't be late.

I view participation & reading responses as the most important single component of your learning experience and will consider the quantity, but mostly the *quality* of your contributions to class discussions. I will publish weekly questions on the readings via ELMS and will carefully read your responses. Be critical, ask questions, engage with previous readings if possible, and assess the quality and significance of the readings you analyze.

Please note that it makes no sense to post a reading response a week or two after we discussed that topic in class. The purpose of these postings is to prepare me and you for our weekly discussion. Posts after our class meeting for the week will not be considered.

You will have 13 sets of questions to respond to (for weeks #2-#14) and can skip one. For each posting you can get a maximum grade of two points. If you have posted your response 12 times (as required) or more, you will get 1 bonus point, bringing this semester-long assignment to 25 points of your final grade. I will grade each posting after each class so you will always know where you stand.

Grading criteria for assessing the quality of your responses include: (1) Have you learned anything new from the readings? (2) where do you agree/disagree with the author? (3) Are you asking critical questions for future discussion on the topic?

Vulnerabilities & Exploits Report: Each student is assigned to a vulnerability type (mobile, Windows, third-party, network) and submits a five-page memo (minimum font size 12, single spaced) on the nature of that type of vulnerability – how has it evolved? What are some of the exploit examples that use this type of vulnerability? Examples of famous hacks that utilized this vulnerability type to create harm (Preferably beyond the examples that were discussed in class), and *five* recommendations on what we can do as a society against such vulnerability type.

Seek sources on this type of vulnerability *beyond* what is assigned in class and become an expert in this type of vulnerability. Grading criteria include – how well you describe this type of vulnerability (6 points), can you attach exploits that utilize this type of vulnerability (6 points), can you list famous hacks that took advantage of this vulnerability type (6 points), are you providing quality recommendations on how to address it as a society? (7 points).

Hacking & Threat Intelligence: Choose two hacking groups from here: https://attack.mitre.org/groups/ (consider this resource as well: https://thedfirreport.com/) and technically compare their campaigns. Visualize their techniques according to the different phases of the hack and put together a report that signals a deep technical understanding of the groups' operations across the different campaigns (no page limit on this one). Conclude with your comparison of the similarities and differences in the way the groups work (come up with your own categories of comparison based on the data you collected!). I expect to see diagrams with arrows that will allow the reader to follow the process of the campaign(s) for each group and a comparative table based on similarities and differences between the groups. Grading criteria include – how well you unpack & visualize the hacking process in each campaign - what was the attack vector, what was the goal of the campaign, what vulnerabilities & exploits were used to execute the hacking campaign, how one phase led to the other (16 points); how insightful is your comparison table between the groups – were you able to technically differentiate between their actions? (9 points). Please make sure you are choosing different groups from one another so we can learn about additional groups during class presentations later in the semester.

Cybersecurity Governance: Based on the threat groups and campaigns analyzed in the previous assignment, identify places of intervention that could be addressed by one/more governance tools (top-down or bottom-up) and provide a detailed report on how each group could have been stopped, if we had those measures in place. Choose top-down/bottom-up governance strategies relevant to your analyzed hacking campaigns, find at least five sources to gain a deeper understanding on your chosen governance strategies, and analyze their pros and cons, areas of coverage, incentive structure in place for their application, and concrete recommendations for US policymakers on how to make them viable.

The 'Hacking & Threat Analysis' and 'Cybersecurity Governance' reports will be jointly presented by you on the last day of the class (Dec 3rd).

Grading criteria include: how creative you are in recognizing potential areas of interventions to stop the hacking campaigns you analyzed (7 points), how well do you explain & justify your chosen governance strategy for these intervention points and able to list the pros and cons for the implementation of your suggested measures (10 points), the quality and feasibility of your recommendations to US policymakers on how to make your chosen governance instruments viable against the hacking campaigns you've analyzed (8 points). The report shouldn't be more than 10 pages, single-spaced, with a minimum font size of 12.

Final grade cutoffs are below:

Final Grade Cutoffs									
+	97.00%	+	87.00%	+	77.00%	+	67.00%		
A	94.00%	B	84.00%	C	74.00%	D	64.00%	F	<60.0%
-	90.00%	-	80.00%	-	70.00%	-	60.00%		

Review of Graded Material

I aim to grade all assignments within 2-3 weeks of their due date and post those grades to ELMS. I try very hard to evaluate each assignment fairly, but I can only evaluate what you submit. I do not have the benefit of knowing all of the time and effort you have put into an assignment. Therefore, you need to make that effort stand out.

Because there may be times when I misinterpret what you have written, I am always willing to clarify how I graded your assignment. If you have any questions about a grade you received, you have **two weeks** from receipt of the grade to contact me (in class, through a meeting, or via email) to discuss your grade. After two weeks have passed, that grade is "locked" and I will not re-evaluate it. Before asking me to review an assignment, however, it is important that you carefully read the feedback and grade justification I have provided.

Extensions

Timelines are essential for graduate work, and extensions will only be available during personal emergencies. If you need to request an extension, you must discuss the matter **in advance** with me. If an extension is granted, the work must be submitted within the extension period to avoid grade penalties. Unexcused delays in submission of the paper will result in a deduction of a letter grade for each day the paper is late, while unexcused delays in presentations will result in a deduction of a letter grade for each class meeting the presentation is late.

Late Work

Unless approved in advance of the due date, late work will automatically be graded down by one step (i.e., 5%) for each day it is late (unless otherwise noted in the syllabus). For example, an assignment that would normally receive an A- if submitted on time would receive a B if it was submitted two days late. Assignments submitted more than one week late will not be accepted.

Attendance and Expectations of Student Participation

The class meets once a week. The course will include lecture, discussion, and group work. It is essential that you participate in the discussions on course materials. Participation means active involvement in class discussions. Students are expected to question, challenge, argue, and discuss issues and topics related to that session's readings.

Regular attendance and participation in this class **is the best way** to grasp the concepts and principles being discussed. However, in the event that a class must be missed due to an illness, you should make a reasonable effort to notify me in advance of the class. If you are absent more than two times due to illness, please schedule a time to meet with me to discuss plans for make-up work. If you are absent on days when papers are due, you are generally expected to still submit the assignment electronically by the due date. Please see the extensions policy below if extra time is needed due to illness. I expect all students to attend all our sessions. It is very important for the learning process. In case you cannot make it, please let me know in advance and we will see what we can do. If you have to miss a session, please make sure you are not missing more than one.

It is also very important that you **will not** be late for class. Respect your peers that show up on time and respect your own learning experience. Being more than 15 minutes late will be considered as an absence. If you have to be late, please let me know in advance.

Tips for Success in Our Course

1. **Participate.** Discussions and group work are a critical part of the course. You can learn a great deal from discussing ideas and perspectives with your peers and professor. Participation can also help you articulate your thoughts and develop critical thinking skills.
2. **Manage your time.** Make time for your participation in discussions each week. Give yourself plenty of time to complete assignments including extra time to handle any technology related problems.
3. **Login regularly.** Log in to ELMS-Canvas several times a week to view announcements, discussion posts and replies to your posts. You may need to log in multiple times a day when group submissions are due.
4. **Do not fall behind.** This class moves at a quick pace and each week builds on the previous one. It will be hard to keep up with the course content if you fall behind in the pre- or post- class work.
5. **Use ELMS-Canvas notification settings.** Canvas ELMS-Canvas can ensure you receive timely notifications in your email or via text. Be sure to enable announcements to be sent instantly or daily.
6. **Ask for help if needed.** If you need help with ELMS-Canvas or other technology, IT Support. If you are struggling with a course concept, reach out to me, and your classmates, for support.

UMD Policies and Resources for Graduate Courses

It is our shared responsibility to know and abide by the University of Maryland's policies that relate to all courses, which include topics like:

- Academic integrity
- Student and instructor conduct
- Accessibility and accommodations
- Copyright and intellectual property

Please visit www.ugst.umd.edu/courserelatedpolicies.html for the Office of Undergraduate Studies' full list of campus-wide policies and follow up with me if you have questions.

Academic Integrity for INST771 – Foundations of Cybersecurity

Academic dishonesty is a corrosive force in the academic life of a university. It jeopardizes the quality of education and depreciates the genuine achievements of others. Apathy or acquiescence in the presence of academic dishonesty is not a neutral act. All members of the University Community—students, faculty, and staff—share the responsibility to challenge and make known acts of apparent academic dishonesty.

You have a responsibility to familiarize themselves with violations of the Code of Academic Integrity. Among these include:

1. **Cheating:** "Intentionally using or attempting to use unauthorized materials, information, or study aids in any academic exercise."
2. **Fabrication:** "Intentional and unauthorized falsification or invention of any information or citation in an academic exercise."
3. **Facilitating Academic Dishonesty:** "Intentionally or knowingly helping or attempting to help another to commit an act of academic dishonesty."

4. **Plagiarism:** "Intentionally or knowingly representing the words or ideas of another as one's own in an academic exercise."

For further clarification or information on the Code of Academic Integrity: http://www.studenthonorcouncil.umd.edu/code.html

Names/Pronouns and Self-Identifications

The University of Maryland recognizes the importance of a diverse student body, and we are committed to fostering inclusive and equitable classroom environments. I invite you, if you wish, to tell us how you want to be referred to both in terms of your name and your pronouns (he/him, she/her, they/them, etc.). The pronouns someone indicates are not necessarily indicative of their gender identity. Visit trans.umd.edu to learn more.

Additionally, how you identify in terms of your gender, race, class, sexuality, religion, and dis/ability, among all aspects of your identity, is your choice whether to disclose (e.g., should it come up in classroom conversation about our experiences and perspectives) and should be self-identified, not presumed or imposed. I will do my best to address and refer to all students accordingly, and I ask you to do the same for all of your fellow Terps.

Communication with Instructor

Email: If you need to reach out and communicate with me, please email me at sevilla@umd.edu. Please DO NOT email me with questions that are easily found in the syllabus or on ELMS (i.e. When is this assignment due? How much is it worth? etc.) but please DO reach out about personal, academic, and intellectual concerns/questions.
I will do my best to respond to emails within 24 hours.

ELMS: I will send important announcements via ELMS messaging. You must make sure that your email & announcement notifications (including changes in assignments and/or due dates) are enabled in ELMS so you do not miss any messages. You are responsible for checking your email and Canvas/ELMS inbox with regular frequency.

Communication with Peers

With a diversity of perspectives and experience, we may find ourselves in disagreement and/or debate with one another. As such, it is important that we agree to conduct ourselves in a professional manner and that we work together to foster and preserve a virtual classroom environment in which we can respectfully discuss and deliberate controversial questions.

I encourage you to confidently exercise your right to free speech—bearing in mind, of course, that you will be expected to craft and defend arguments that support your position. Keep in mind, that free speech has its limits, and this course is NOT the space for hate speech, harassment, and derogatory language. I will make every reasonable attempt to create an atmosphere in which each student feels comfortable voicing their argument without fear of being personally attacked, mocked, demeaned, or devalued.

Any behavior (including harassment, sexual harassment, and racially and/or culturally derogatory language) that threatens this atmosphere will not be tolerated. Please alert me immediately if you feel threatened, dismissed, or

silenced at any point during our semester together and/or if your engagement in discussion has been in some way hindered by the learning environment.

Course Outline

Module	Session #	Topic	Deliverable
1: **Intro to Cybersecurity:** How to get started? Where are the incentives? How can policymakers address tech problems?	**1 (Aug 27th)**	Get to know the class, your peers, and the problem(s) we will tackle. An 'Introduce yourself' exercise. - **Take** the cybersecurity quiz - please report to the class about one finding from the quiz that surprised you https://www.pewinternet.org/quiz/cybersecurity-knowledge We will discuss the goals of the class and go over the syllabus. **Read**: Spitzner, 2021 - "Getting started with cybersecurity with a non-technical background." SNAS Blog, January 18, 2021 https://www.sans.org/blog/getting-started-in-cybersecurity-with-a-non-technical-background/ **Listen:** "The Economics of Cybersecurity." *Malicious Life Podcast* https://malicious.life/episode/episode-215/ --- **Optional Read**: Anderson and Moore, 2009 – "Information security: where computer science, economics and psychology meet" *Phil. Trans. R. Soc. A (2009) 367, 2717–2727* doi:10.1098/rsta.2009.0027 https://royalsocietypublishing.org/doi/pdf/10.1098/rsta.2009.0027 **Optional Read**: Bruce Schneier, 2020, "Technologists vs. Policy Makers." IEEE Security & Privacy (Volume: 18, Issue: 1, Jan.-Feb. 2020) https://ieeexplore.ieee.org/document/8965265	
2: **Vulnerabilities, Weaknesses & Exploits** The technical roots of cyber-insecurity	**2 (Sept. 3rd)**	Introduction to the concepts of vulnerabilities, weaknesses, and exploits **Watch:** Intro to CVE - https://www.youtube.com/watch?v=F06P89V6sDI **Watch:** Where is vulnerability information found? https://www.youtube.com/watch?v=bEKmTJPSZgs **Watch**: Exploiting Vulnerabilities: https://www.youtube.com/watch?v=pdhmjeT8780 **Watch**: The Vulnerability life-cycle: https://www.youtube.com/watch?v=9203OvYjksQ **Read:** Wright (2024). "10 of the biggest zero-day attacks of 2023." *Techtarget.com*	

		https://www.techtarget.com/searchsecurity/feature/10-of-the-biggest-zero-day-attacks-of-2023 **Read:** O'Neill (2021), "2021 has broken the record for zero-day hacking attacks" Technology Review, September 23 2021 https://www.technologyreview.com/2021/09/23/1036140/2021-record-zero-day-hacks-reasons/ **Watch:** What is Common Weakness Enumeration (CWE)? https://www.youtube.com/watch?v=GJNaEpv3Ok0 **Explore:** 2023 CWE Top 25 Most Dangerous Software Weaknesses https://cwe.mitre.org/top25/archive/2023/2023_top25_list.html **Explore:** Known Exploited Vulnerabilities Catalog https://www.cisa.gov/known-exploited-vulnerabilities-catalog **Read:** The Future of Vulnerabilities Equities Processes Around the World https://www.lawfaremedia.org/article/future-vulnerabilities-equities-processes-around-world **Read:** Herr, Schneier, Morris (2017) "Taking Stock: Estimating Vulnerability Re-discovery." Cybersecurity Project, Belfer Center https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2928758 **Read:** Pauley et al. (2023). 'The CVE Wayback Machine: Measuring Coordinated Disclosure from Exploits against Two Years of Zero-Days.' *IMC '23: Proceedings of the 2023 ACM on Internet Measurement Conference* https://dl.acm.org/doi/abs/10.1145/3618257.3624810 --- **(Optional) Listen:** How CVE, CISA and NIST work together to manage vulnerabilities– https://www.youtube.com/watch?v=MIoV_X18DvE&t=1s **(Optional) Watch**: State of the CVE Program https://www.youtube.com/watch?v=ISVyBgIWF1c **(Optional) Read:** Dullien, T. (2017) 'Weird Machines, Exploitability, and Provable non-Exploitability', IEEE Transactions on Emerging Topics in Computing: https://www.computer.org/csdl/journal/ec/2020/02/08226852/13rRUx0xPx6	

	3 (Sept. 10th)	Mobile (iOS & Android), MS Windows **Read:** Ian Beer & Samuel Groß, 2021, "A deep dive into an NSO zero-click iMessage exploit: Remote Code Execution." *Google Project Zero*, December 15 2021 https://googleprojectzero.blogspot.com/2021/12/a-deep-dive-into-nso-zero-click.html **Read:** Huasong Meng, Vrizlynn L.L. Thing, Yao Cheng, Zhongmin Dai, Li Zhang, 2018, "A survey of Android exploits in the wild." *Computers & Security* 76, pp. 71-91 https://ycheng.cc/assets/docs/2018-A%20survey%20of%20Android%20exploits%20in%20the%20wild.pdf **Read**: Unraveling EternalBlue: inside the WannaCry's enabler https://cybernews.com/security/eternalblue-vulnerability-exploit-explained/ **Read:** Brian Krebs, 2024, Six 0-Days Lead Microsoft's August 2024 Patch Push https://krebsonsecurity.com/2024/08/six-0-days-lead-microsofts-august-2024-patch-push/	
	4 (Sept. 17th)	Third Party-Software – 'The Supply Chain Problem' (SolarWinds, Log4J, Heartbleed, ShellShock, XZ Utils); Open vs. Closed source software **Read:** Brian Krebs, 2018, "Supply Chain Security is the Whole Enchilada, But Who's Willing to Pay for It?" Krebsonsecurity.com, Oct 5 2018- https://krebsonsecurity.com/2018/10/supply-chain-security-is-the-whole-enchilada-but-whos-willing-to-pay-for-it/ **Read**: Backdoor in XZ Utils That Almost Happened https://www.lawfaremedia.org/article/backdoor-in-xz-utils-that-almost-happened?s=03 **Read:** Robert Chesney**,** 2021, **"**SolarWinds and the Holiday Bear Campaign: A Case Study for the Classroom." *Lawfareblog.com,* August 25 2021 https://www.lawfareblog.com/solarwinds-and-holiday-bear-campaign-case-study-classroom **Read:** Kim Zetter, 2023, "The Untold Story of the Boldest Supply-Chain Hack Ever" *Wired.com* https://www.wired.com/story/the-untold-story-of-solarwinds-the-boldest-supply-chain-hack-ever/ **Read:** The Heartbleed vulnerability – https://heartbleed.com/	

		Read: Stone, 2020, 'Shellshock In-Depth: Why This Old Vulnerability Won't Go Away' *securityintelligence.com,* August 6 2020 https://securityintelligence.com/articles/shellshock-vulnerability-in-depth/ **Read:** Torres-Arias, 2021, **"**What is Log4j? A cybersecurity expert explains the latest internet vulnerability, how bad it is and what's at stake" https://theconversation.com/what-is-log4j-a-cybersecurity-expert-explains-the-latest-internet-vulnerability-how-bad-it-is-and-whats-at-stake-173896 **Read**: Ford. (2007). Open vs. Close – Which Source is more secure? https://dl.acm.org/doi/pdf/10.1145/1217256.1217267 **Optional Read:** Newman, 2021, "The Log4J Vulnerability Will Haunt the Internet for Years." December 13 2021 https://www.wired.com/story/log4j-log4shell/ **Optional Read:** Ross Anderson, 2002, "Security in Open versus Closed Systems – The Dance of Boltzmann, Coase and Moore" https://www.cl.cam.ac.uk/~rja14/Papers/toulouse.pdf	
	5 (Sept. 24th)	Network Vulnerabilities - Background on networking, the Internet & network security **Read:** What is a packet? Mar 30, 2021: https://computer.howstuffworks.com/question525.htm **Read:** Oracle, 2010, 'Data Encapsulation and the TCP/IP Protocol Stack' *Oracle.com* https://docs.oracle.com/cd/E19455-01/806-0916/ipov-32/ **Read:** Andy O'Donnell, 2021, "What Are Packet Sniffers and How Do They Work?" June 25 2021 https://www.lifewire.com/what-is-a-packet-sniffer-2487312 **Read:** Checkpoint, Firewall History: https://www.checkpoint.com/cyber-hub/network-security/what-is-firewall/ **Read**: Stateful vs. Stateless Firewalls https://www.cdw.com/content/cdw/en/articles/security/stateful-versus-stateless-firewalls.html **Read:** Pieter Arntz, 2021, "How a VPN can protect your online privacy", May 12 2021 https://blog.malwarebytes.com/privacy-2/2021/01/how-a-vpn-can-protect-your-online-privacy/ **Explore:** The TOR Project - https://www.torproject.org/	

		Read: Craig Timberg, 2015, "Internet protocol from 1989 leaves data vulnerable to hijackers," *Washingtonpost.com* May 31 2015 https://www.washingtonpost.com/sf/business/2015/05/31/net-of-insecurity-part-2/ **Read:** Brian Krebs, 2021, What Happened to Facebook, Instagram, & WhatsApp? *Kerbsonsecurity.com*, Oct 4 2021 https://krebsonsecurity.com/2021/10/what-happened-to-facebook-instagram-whatsapp/ **Read:** Leiner et al. 2009. "A Brief History of the Internet" *ACM SIGCOMM Computer Communication Review* 22 Volume 39, Number 5 https://sites.cs.ucsb.edu/~almeroth/classes/F10.176A/papers/internet-history-09.pdf **Watch:** The underwater cables of the Internet https://www.youtube.com/watch?v=Ve810FHZ1CQ&t=11s **Optional Read:** Perta et al. 2015. "A Glance through the VPN Looking Glass: IPv6 Leakage and DNS Hijacking in Commercial VPN clients" https://www.petsymposium.org/2015/papers/02_Perta.pdf	
	6 (Oct. 1st)	Categorizing Events & Measuring the severity of cyber-based vulnerabilities – CVSS & EPSS **Watch:** CVSS - https://www.youtube.com/watch?v=x3wAINJF7UE **Watch:** What is the Common Vulnerability Scoring System (CVSS)? https://nucleussec.com/blog/vulnerability-management-and-cvss/ **Watch:** EPSS - https://www.youtube.com/watch?v=9Pzye4d-Hq4 **Read:** Jacobs et al. 2023. "Enhancing Vulnerability Prioritization: Data-Driven Exploit Predictions with Community-Driven Insights" *IEEE European Symposium on Security and Privacy Workshops* https://ieeexplore.ieee.org/document/10190703 **Read:** Wunder et al. (2024). "Shedding Light on CVSS Scoring Inconsistencies: A User-Centric Study on Evaluating Widespread Security Vulnerabilities" *IEEE Symposium on Security and Privacy (S&P)* https://arxiv.org/abs/2308.15259 **Read:** Harry, C., Sivan-Sevilla, I., McDermott (2025). Measuring the size and severity of the integrated cyber attack surface across US county governments. *Journal of Cybersecurity* *https://academic.oup.com/cybersecurity/article/11/1/tyae032/7959399* ---	

		Optional Read: Mell & Spring, (2022), "Measuring the Common Vulnerability Scoring System Base Score Equation" *NIST* https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8409.pdf **Optional Read:** Allodi et al. 2018. "Identifying Relevant Information Cues for Vulnerability Assessment Using CVSS." *CODASPY '18: Proceedings of the Eighth ACM Conference on Data and Application Security and Privacy* https://arxiv.org/pdf/1803.07648.pdf	
3**: Hacking & Threat Intelligence:** The MITRE Framework, Threat Intelligence, The Diamond Model.	**7 (Oct. 8th)**	The Hacking Process – How hackers work and a glimpse into the 'hacker culture' **Read:** The Hacker Manifesto, 1986: https://www.askapache.com/hacking/hacker-manifesto/ **Read:** Michael Buckbee, 2023, What is The Cyber Kill Chain and How to Use it Effectively | Varonis: https://www.varonis.com/blog/cyber-kill-chain **Watch:** The MITRE ATT&CK Framework https://www.youtube.com/watch?v=Yxv1suJYMI8 **Explore**: The MITRE ATT&CK Matrix https://attack.mitre.org/ **Read**: 10 Cases about Hacking that everybody should know https://blog.ipleaders.in/10-cases-about-hacking-that-everybody-should-know/ **Watch:** Elazari, 2014, 'hackers: the internet's immune system' https://www.ted.com/talks/keren_elazari_hackers_the_internet_s_immune_system **Read:** Greenberg, 2023, "The Mirai Confessions: Three Young Hackers Who Built a Web-Killing Monster Finally Tell Their Story" https://www.wired.com/story/mirai-untold-story-three-young-hackers-web-killing-monster/ Story is also available here in case subscription is required. https://www.cisa.gov/sites/default/files/2024-09/FY23_RVA_Analysis_508.pdf	**Vulnerabilities & Exploits Report is due**
	8 (Oct. 15th)	Threat Intelligence – Intrusion Detection, Honeypots, DoD's diamond model and Threat Data **Read:** Pennington et al. (2019). "Getting started with ATT&CK" *MITRE* https://www.mitre.org/sites/default/files/2021-11/getting-started-with-attack-october-2019.pdf	

		Read: A. L. Buczak and E. Guven, "A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection," in *IEEE Communications Surveys & Tutorials*, vol. 18, no. 2, pp. 1153-1176, Secondquarter 2016. https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7307098 **Read**: What is a Honeypot? https://www.kaspersky.com/resource-center/threats/what-is-a-honeypot **Explore:** The HoneyNet Project: https://www.honeynet.org/ **Read:** Britton et al. (2018). "Analysis of 24 Hours Internet Attacks" https://www.honeynet.org/papers/THP-Paper-Bots_Keep_Talking_To_Us.pdf **Read:** Li et al. (2019). "Reading the Tea leaves: A Comparative Analysis of Threat Intelligence" *The 28th USENIX Security Symposium* https://www.usenix.org/system/files/sec19-li-vector_guo.pdf **Read:** Caltagirone et al. (2013). The Diamond Model of Intrusion Analysis. *US Department of Defense* https://apps.dtic.mil/sti/pdfs/ADA586960.pdf **Read:** Lennart Maschmeyer, Ronald J. Deibert, and Jon R. Lindsay, 2021, "A tale of two cybers - how threat reporting by cybersecurity firms systematically underrepresents threats to civil society:" Journal Of Information Technology & Politics 2021, Vol. 18, No. 1, 1–20 https://www.tandfonline.com/doi/full/10.1080/19331681.2020.1776658 **Read:** Harry, C., & Gallagher, N. W. (2023). Categorizing cyber effects. In *The Elgar Companion to Digital Transformation, Artificial Intelligence and Innovation in the Economy, Society and Democracy* (pp. 7-31). Edward Elgar Publishing. Chapter is available here.	
4**: The Threat Landscape:** Nation States & Criminal Groups: Ransomware, Darknet, Bitcoin, Commercial Spyware, Critical Infrastructures, Economic Espionage,	**9 (Oct. 22nd)**	Nation States - Government Surveillance, Economic Espionage, Commercial Spyware, Critical Infrastructures, Cyber-enabled disinformation *Government Surveillance* **Read:** Baker, 2019, "Rethinking Encryption" *Lawfare* https://www.lawfaremedia.org/article/rethinking-encryption **Read:** Baker and Landau, 2019, "New Perspectives on the Future of Encryption" *Lawfare* https://www.lawfaremedia.org/article/new-perspectives-future-encryption	

Cyber-enabled disinformation		**Read:** https://lpeproject.org/blog/social-media-authoritarianism-and-the-world-as-it-is/ *Economic Espionage* **Read:** Adam Segal, 2016, "Why China Hacks the World," *The Christian Science Monitor,* January 31 2016 https://www.csmonitor.com/layout/set/amphtml/World/Asia-Pacific/2016/0131/Why-China-hacks-the-world **Read:** https://www.judiciary.senate.gov/imo/media/doc/12-12-18%20Priestap%20Testimony.pdf **Optional Read:** https://www.cfr.org/report/threat-chinese-espionage *Commercial Spyware* **Watch:** Global Spyware Scandal: Exposing Pegasus (Parts 1 & 2) *PBS.org* https://www.pbs.org/wgbh/frontline/documentary/global-spyware-scandal-exposing-pegasus/ **Read:** Ronald J. Deibert (2022) "The Autocrat in your iPhone" *Foreign Affairs* https://www.foreignaffairs.com/world/autocrat-in-your-iphone-mercenary-spyware-ronald-deibert Essay is available here in case you have access problems. **Optional Watch:** "Digital Subversion: The Threat to Democracy" | 18th Annual Seymour Martin Lipset Lecture - https://www.youtube.com/watch?v=vxxlgrTyI-M *Critical Infrastructures* **Read:** Johnson, 2021, "Cyberattacks on our energy infrastructure: The need for a national response to a national security threat" *Atlantic Council* https://www.atlanticcouncil.org/blogs/energysource/cyberattacks-on-our-energy-infrastructure/ **Read:** Microsoft Threat Intelligence. 2023. "Volt Typhoon targets US critical infrastructure with living-off-the-land techniques" https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/ **Read:** JD Work and Richard Harknett, 2020	

		"Troubled Vision: Understanding recent Israeli-Iranian offensive cyber exchanges." *The Atlantic Council* https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/troubled-vision-understanding-israeli-iranian-offensive-cyber-exchanges/ **Watch:** Treatment Plant Intrusion – Press Conference – Attacking water infrastructure in Florida https://www.youtube.com/watch?v=MkXDSOgLQ6M **Read:** https://media.defense.gov/2023/May/24/2003229517/-1/-1/0/CSA_Living_off_the_Land.PDF **Optional Read:** Zetter, 2016, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," *wired.com,* March 3 2016 https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/ *Cyber-enabled disinformation* **Watch:** Laura Galante, 2017, "How (and why) Russia hacked the US election" *Ted.com* https://www.ted.com/talks/laura_galante_how_and_why_russia_hacked_the_us_election **Read**: Jennifer S Hunt. (2021). "Countering cyber-enabled disinformation: implications for national security." *Australian Journal of Defence and Strategic Studies* https://research-management.mq.edu.au/ws/portalfiles/portal/174550015/Publisher_version.pdf	
	10 (Oct. 29th)	Cyber Criminals – Cryptocurrency & Ransomware & Darknet Markets **Watch:** But how does Bitcoin really work? https://www.youtube.com/watch?v=bBC-nXj3Ng4 **Read**: Narayanan et al. (2016), "Bitcoin and Cryptocurrency Technologies," Introduction (pp. 2 – 22) https://d28rh4a8wq0iu5.cloudfront.net/bitcointech/readings/princeton_bitcoin_book.pdf **Read:** De Vynck, Lerman, Nakashima, and Alcantara, 2021, "The Anatomy of Ransomware Attack," *washingtonpost.com,* July 9 2021 https://drive.google.com/file/d/1R8-qNqDiNVEcvG4zELuEBWmQxA0AaSov/view?usp=sharing **Read:** Institute for Security & Technology. 2021. "Combating Ransomware: A Comprehensive Framework for Action – Key	

		Recommendations from the Ransomware Task Force." *Institute for Security and Technology* https://securityandtechnology.org/wp-content/uploads/2021/04/IST-Ransomware-Task-Force-Report.pdf **Read:** Jenny Jun, 2021, "The Political Economy of Ransomware" *Warontherocks.com*, June 2 2021 https://warontherocks.com/2021/06/the-political-economy-of-ransomware/ **Read:** Razaulla et al. (2023). "The Age of Ransomware: A Survey on the Evolution, Taxonomy, and Research Directions" *IEEE Access* https://drive.google.com/file/d/1XoJrhUS0JSTCRKYzCSt2-kC9N1Y8IMyf/view?usp=sharing **Read:** Meland et al. 2020 "The Ransomware-as-a-Service economy within the darknet" *Computers & Security* Vol. 92 https://www.sciencedirect.com/science/article/pii/S0167404820300468	
5: **Cybersecurity Governance:** Policy Strategies, Cybersecurity Regulations, Cyber Insurance, Bug Bounty Programs, Cyber Norms	**11 (Nov. 5th)**	Top-down Doctrines for cybersecurity - Policy Strategies **Read:** Mulligan D. and F. Schneider. (2011). 'Doctrine for Cybersecurity' *Daedalus* Vol. 140, No. 4, Protecting the Internet as a Public Commons (Fall 2011), pp. 70-92 (23 pages) http://www.cs.cornell.edu/fbs/publications/publicCybersecDaed.pdf **Read:** Eviatar Matania, Lior Yoffe & Michael Mashkautsan, A Three-Layer Framework for a Comprehensive National Cyber-Security Strategy, 17 GEO. J. INT'l AFF. 77 (2016). https://www.jstor.org/stable/26395977 **Read:** O'Neill, 2022, "Inside the plan to fix America's never-ending cybersecurity failures" *MIT Technology Review* https://www.technologyreview.com/2022/03/18/1047395/inside-the-plan-to-fix-americas-never-ending-cybersecurity-failures/ **Read**: CSC Report – Executive Summary https://drive.google.com/file/d/1c1UQI74Js6vkfjUowI598NjwaHD1YtlY/view **Optional Read:** Swire P., 2018, "A pedagogic Cybersecurity Framework" *Communications of the ACM* Volume 61 Issue 10 pp 23–26 https://dl.acm.org/doi/10.1145/3267354 **Option Read:** Ross Anderson, 2001, "Why Information Security is Hard - An Economic Perspective." https://www.acsac.org/2001/papers/110.pdf **Optional Read:** Nye, 2014, "The Regime Complex for Managing Global Cyber Activities," *The Centre for International Governance Innovation*	**Hacking & Threat Intelligence Report is due**

		and the Royal Institute for International Affairs https://www.cigionline.org/sites/default/files/gcig_paper_no1.pdf	
	12 (Nov. 12th)	Top-down Doctrines for cybersecurity - Government Regulation Guest talk by Dr. Gregory Von Lehmen **Read:** Jim Dempsey. (2022). "Cybersecurity Regulation: It's Not 'Performance-Based' If Outcomes Can't Be Measured" *Lawfare* https://www.lawfaremedia.org/article/cybersecurity-regulation-its-not-performance-based-if-outcomes-cant-be-measured **Read:** The GaTech Professor who didn't comply: https://www.internetgovernance.org/2024/08/27/the-justice-department-sues-georgia-tech-a-teachable-moment-in-cybersecurity-management/ Enforcement of cybersecurity regulations: **Read:** https://www.lawfaremedia.org/article/enforcement-cybersecurity-regulations-part-1 https://www.lawfaremedia.org/article/enforcement-cybersecurity-regulations-part-2 https://www.lawfaremedia.org/article/enforcement-cybersecurity-regulations-part-3	
	13 (Nov. 19th)	Bottom-up governance mechanisms – Norms, Property Rights, Cyber Insurance, Bug Bounty Programs **Read:** Martha Finnemore and Duncan Hollis, 2017, "Constructing Norms for Global Cybersecurity," American Journal of International Law, Volume 110 , Issue 3 , July 2016 , pp. 425 - 479 DOI: https://doi.org/10.1017/S0002930000016894 **Read:** Van Eeten, M. (2017). 'Patching Cyebrsecurity Governance: an empirical view of emergent governance mechanisms for cybersecurity.' *Digital Policy, Regulation and Governance* Volume 19 Issue 6 https://www.emerald.com/insight/content/doi/10.1108/DPRG-05-2017-0029/full/pdf?title=patching-security-governance-an-empirical-view-of-emergent-governance-mechanisms-for-cybersecurity **Read:** Daniel W. Woods and Tyler Moore. 2019. "Does Insurance Have a Future in Governing Cybersecurity?" *IEEE Security & Privacy* (Volume: 18, Issue: 1) https://ieeexplore.ieee.org/abstract/document/8833500 **Listen:** Lawfare Daily: Katie Moussouris on Bug Bounties – Aug 12 2024	

		https://www.lawfaremedia.org/article/lawfare-daily--katie-moussouris-on-bug-bounties **Listen:** Malicious Life – Why aren't there more bug bounty programs? https://podcastaddict.com/malicious-life/episode/161821804 **Optional Read:** Ryan Ellis & Yuan Stevens, 2022, "Bounty Everything" *Data & Society*, January 12 2022 https://datasociety.net/library/bounty-everything-hackers-and-the-making-of-the-global-bug-marketplace/ **Optional Read:** Jukka Ruohonen and Luca Allodi, 2018, A Bug Bounty Perspective on the Disclosure of Web Vulnerabilities, *WEIS 2018* https://weis2018.econinfosec.org/wp-content/uploads/sites/5/2018/05/WEIS_2018_paper_33.pdf	
	14 (Nov. 26th)	No Class! Options include **Quantum Computing** – https://dl.acm.org/doi/pdf/10.1145/3571725 - Feel free to suggest more!	
	15 (Dec. 3th)	Class presentations of both reports – hacking campaigns and required governance measures (cake is on me!)	**Cybersecurity Governance report & Presentations are due**

Note: This is a tentative schedule, and subject to change as necessary – monitor the course ELMS page for current deadlines. In the unlikely event of a prolonged university closing, or an extended absence from the university, adjustments to the course schedule, deadlines, and assignments will be made based on the duration of the closing and the specific dates missed.

Resources & Accommodations

Accessibility and Disability Services

The University of Maryland is committed to creating and maintaining a welcoming and inclusive educational, working, and living environment for people of all abilities. The University of Maryland is also committed to the principle that no qualified individual with a disability shall, on the basis of disability, be excluded from participation in or be denied the benefits of the services, programs, or activities of the University, or be subjected to discrimination. The **Accessibility & Disability Service (ADS)** provides reasonable accommodations to qualified individuals to provide equal access to services, programs and activities. ADS cannot assist retroactively, so it is generally best to request accommodations several weeks before the semester begins or as soon as a disability becomes known. Any student who needs accommodations should contact me as soon as possible so that I have sufficient time to make arrangements.

For assistance in obtaining an accommodation, contact Accessibility and Disability Service at 301-314-7682, or email them at **adsfrontdesk@umd.edu**. Information about **sharing your accommodations with instructors**, **note taking assistance** and more is available from the **Counseling Center**.

Student Resources and Services

Taking personal responsibility for your own learning means acknowledging when your performance does not match your goals and doing something about it. I hope you will come talk to me so that I can help you find the right approach to success in this course, and I encourage you to visit **UMD's Student Academic Support Services website** to learn more about the wide range of campus resources available to you.

In particular, everyone can use some help sharpening their communication skills (and improving their grade) by visiting **UMD's Writing Center** and schedule an appointment with the campus Writing Center.

You should also know there are a wide range of resources to support you with whatever you might need (**UMD's Student Resources and Services website** may help). If you feel it would be helpful to have someone to talk to, visit **UMD's Counseling Center** or **one of the many other mental health resources on campus**.

Basic Needs Security

If you have difficulty affording groceries or accessing sufficient food to eat every day, or lack a safe and stable place to live, please visit **UMD's Division of Student Affairs website** for information about resources the campus offers you and let me know if I can help in any way.

Technology Policy

Please refrain from using cellphones, laptops, and other electronic devices during class sessions unless we have designated such use as part of a class exercise.

Course Evaluation

Please submit a course evaluation through CourseEvalUM in order to help faculty and administrators improve teaching and learning at Maryland. All information submitted to CourseEvalUM is confidential. Campus will notify you when CourseEvalUM is open for you to complete your evaluations for fall semester courses. Please go directly to the **Course Eval UM website** to complete your evaluations. By completing all of your evaluations each semester, you will have the privilege of accessing through Testudo, the evaluation reports for the thousands of courses for which 70% or more students submitted their evaluations.