HARVARD Kennedy School

Updated: 8 Oct 2025
IGA-236: Cybersecurity: Technology, Policy, and Law
Harvard Kennedy School
Spring 2026
Mondays and Wednesdays • 9:00 – 10:15 AM • Starr Auditorium (Belfer 200)
Optional Fridays (as announced) • 3:00 – 4:15 PM • Wex-463

Instructor:

Simson Garfinkel
sgarfinkel@fas.harvard.edu
Office: TBD

Course Assistants:

TBD

Faculty Assistant:

Karin Vander Schaaf (she/her)
karin_vander_schaaf@hks.harvard.edu
617-496-5584
Office: Belfer 313

Canvas:

TBD

Office Hours Schedule

Office hours are generally by appointment. I am happy to discuss the class, the assignments, your other projects, your future careers, and any other topic in cybersecurity, privacy, and related policies. Please email me at sgarfinkel@fas.harvard.edu for an appointment.

Course Description

Cybersecurity is now a primary concern of governments, NGOs, corporations and ordinary citizens. Criminals wielding ransomware have shut down pipelines, airports and hospitals. Governments have hacked cellphones of journalists and protesters. Academics have shown how to wirelessly take over a car and force it off the road. Dozens of organizations are collecting your personal data.

Cybersecurity is complex, touching upon personal freedom, public safety, corporate behavior, international relations, and war. This course explores that interplay. Designed for those who have no background in computer science, this course presents enough technology so that you won't feel lost, with hands on labs that should be readily accessible to all. We then dive deeper, analyzing the complex, social, political and economic factors that shape cybersecurity realities.

Cybersecurity is international, and this course will study cases from the US, Europe, China and Latin America. Students will help us achieve global reach by analyzing, discussing and presenting these complex topics in a variety of formats, including posters, presentations and short videos.

Course Learning Goals and Objectives

This course aims to give you the necessary tools to understand legal and policy issues in cyberspace. While it is impossible to become a cybersecurity expert in a single semester, you will leave the course as intelligent laypeople, adept at discussing computer and Internet security policy issues and able to spot political agendas disguised as technical arguments. You will understand how technology and policy interrelate, when it's time to turn to technical experts, and how to use technical expertise to form effective policy.

This course is designed for policymakers rather than for implementers of preexisting policy. As such, we will not discuss how to implement specific Internet security laws and regulations. Rather, we will discuss how to effectively determine which policies are the correct ones to mandate: for government, for private industry, and for individuals. This course is less about learning a body of answers, and more about learning to think about these topics in general. After completing this class, you will be more sophisticated when you approach new Internet security policy issues. Specifically, you will be able to weigh pros and cons, examine consequences of policies, and craft and recommend policies of your own.

Eligibility and Prerequisites

This course is open to:

- **Graduate students** from any Harvard school or department
- **Qualified undergraduates** with the permission of the instructor
- **MIT and Tufts Fletcher** cross-registered graduate students on a space-available basis.

KSG fellows whose fellowship does not allowing taking this course for credit are welcome to audit and will be admitted as space allows. No other auditors are allowed.

There are no prerequisites. Prior training in natural or engineering sciences is not a requirement. This class assumes no computer science background. There will be **optional Q&A sessions on some Fridays as my schedule permits** to provide enrichment and discuss topics as they arise.

How This Class Differs from Other HKS Cybersecurity Classes

Harvard Kennedy School offers several classes on cybersecurity topics:

James Waldo teaches IGA-538: "Technology, Privacy, and the Trans-National Nature of the Internet." This class is focused on privacy in the digital age. Privacy and security are necessarily intertwined. Again, while there is some overlap on our two classes, IGA-236 will only touch briefly on privacy concerns and focus primarily on security.

Bruce Schneier teaches IGA-237M: "Future Issues in Cybersecurity Policy." This is a module seminar that meets for six three-hour sessions in the fall semester. The class focuses on a single topic, which changes every year. Previous classes covered blockchain, AI security, and foreign disinformation operations. This class will not be taught in Fall 2026. (Bruce Schneier also taught IGA 236 last year. For a list of what's different, see the end of this document.)

Schedule

```
                          2026
      January                   February                  March
Su Mo Tu We Th Fr Sa   Su Mo Tu We Th Fr Sa   Su Mo Tu We Th Fr Sa
             1  2  3    1  2  3  4  5  6  7    1  2  3  4  5  6  7
 4  5  6  7  8  9 10    8  9 10 11 12 13 14    8  9 10 11 12 13 14
11 12 13 14 15 16 17   15 16 17 18 19 20 21   15 16 17 18 19 20 21
18 19 20 21 22 23 24   22 23 24 25 26 27 28   22 23 24 25 26 27 28
25 26 27 28 29 30 31                          29 30 31
       April                     May
Su Mo Tu We Th Fr Sa   Su Mo Tu We Th Fr Sa
          1  2  3  4                   1  2
 5  6  7  8  9 10 11    3  4  5  6  7  8  9
12 13 14 15 16 17 18   10 11 12 13 14 15 16
19 20 21 22 23 24 25   17 18 19 20 21 22 23
26 27 28 29 30         24 25 26 27 28 29 30
                       31
```

Key: Course Preview Days Class Meetings. Holiday. Exam Week.

May 1 – Full-term courses end

May 18 – Full-term grades due

Class Outline – Week by Week

Class Topic	Textbook reading for Monday	Assignment / Lab Due Sunday 5PM
Jan 22/23 — Course Preview		
Jan 26 What is "Cybersecurity?" **Jan 28** Threat modeling	Assigned articles (see below)	**Canvas Reflect:** Pew
Feb 2 Actors, Terrain and History **Feb 4** Cryptography	**CIC** Introduction **CIC 1**, "What is Cybersecurity?" (31p)	Lab 1 - Decrypt the documents **Briefing Memo** – Cryptography Policy Challenges
Feb 9 Identifying Machines **Feb 11** Identifying People	**CIC 2**, "Technology Basics and Attribution (pp. 60-85; 25p)	Lab 2 – DNS, Traceroute and ping **Canvas Reflect:** DNS, Traceroute and ping
~~**Feb 16**~~ *(President's Day)* **Feb 18** Anonymity	**CIC 2 Cont.**, "Technology Basics and Attribution (pp. 86-108; 22p)	Lab 3 – VPNs and TOR **Canvas SAR:** A cybersecurity incident in a country other than the United States
Feb 23 Human factors **Feb 25** Phishing	**CIC 3**, "Economics and the Human Factor" (30p)	Lab 4 – Threat Inside **Briefing Memo - Phishing**
Mar 2 Threats and Cyber Arms **Mar 4** The VEP debate	**CIC 4**, "The Military and Intelligence Communities" (56p)	**Canvas Reflect:** Your Security Plan

Class Topic	Textbook reading for Monday	Assignment / Lab Due Sunday 5PM
Mar 9 Theory for governments. **Mar 11** Practice for the person	**CIC 5**, "Cybersecurity Theory" (52p)	Lab 5 – Watching Websites Watching You (HTTP Toolkit) **Briefing Memo – Website Trackers***
Mar 16 & 18 — No class — Spring Break		
Mar 23 Surveillance Capitalism **Mar 25** Data Protection	**CIC 6**, "Consumer Protection Law" (32p)	Lab 6 – Have you been pwned? **Group: Cybersecurity Cartoon**
Mar 30 Criminal hacking **Apr 1**	**CIC 7**, "Criminal Law" (52p)	Lab 7 – Gandalf Prompt Hacking **Briefing Memo — AI**
Apr 6 Resilience **Apr 8** AI as Critical Infrastructure	**CIC 8**, "Critical Infrastructure" (34p)	
Apr 13 Intellectual Property **Apr 15** Web scraping and OSINT	**CIC 9**, Intellectual Property Rights" (26p)	Group: **Short Form Video Proposal**
Apr 20 Supply Chain Security **Apr 22**	**CIC 10**, "The Private Sector" (50p)	
Apr 27 Tussle 2 **Apr 29** Tussle 2	**CIC 11**, "Cybersecurity Tussles" (20p)	
May 4 **May 6**	**CIC 12**, "Cybersecurity Futures" (18p)	**Group Short Form Video Due**
Week of May 11	n/a	**Final Assessment: Poster Session**

Key:

CIC— Read the chapter in *Cybersecurity in Context* and come to class with your notes in hand. Your notes should include: 1) *your name* (there is a 20% chance that the notes will be collected for credit); 2) *key points* from the reading that you wish to discuss; 3) *terms* that you want better explained; 4) *objections* that you have to the information that was presented by Hoofnagle and Richard.

Canvas Reflect — Post a personal reflection (1-2 paragraphs) regarding the topic on Canvas and react to the posts of two other students.

Canvas SAR — Post a 2-sentence Significant Activity Report about this topic in the discussion forum. Respond to two other SARs.

Briefing Memo — Briefing memos are 1-page documents that are uploaded to Canvas.

* Note that the Website Trackers Briefing Memo is due on March 22.

Group – There are two group projects in this course. The **Cybersecurity Cartoon** is an editorial or strip cartoon about a cybersecurity topic discussed in class. You will create this with another student and post it to Canvas. The **Short Form Video** is a project for 4-6 students. For this project you will write a proposal for your short form video, including its learning objectives and the details of what equipment you will use, where you will film, and how you will edit. You will then create the video and post it for the class to review.

Lab — Complete the lab, as discussed below

Final Assessment—The final assessment is a poster that you will create with an accompanying 1-page briefing paper. You will present this during the exam week in lieu of a final exam.

Grading and Assignments

This class includes both individual and group assessments.

Individual assessments include:

Your participation in class and on Canvas	20 %
Canvas Reflections and SARs	12 %
Briefing Memos	12 %
Your collected notes (see below)	12 %
Your security poster for the poster session	10 %
The 1-page briefing paper for your poster	9 %
Your 60-second presentation of your poster.	5 %

Group assessments consist of two group projects:

An editorial cartoon on a cybersecurity topic.	10 %
A short-form video (described below)	10 %

Grading

Final grades will be assigned according to the Dean's Recommended Grade distribution (available here).

Most assignments and the collected notes will be graded on a scale of 0-3, where:

0 the assignment was not handed in

+1 The assignment did not reflect significant thought and analysis

+2 The assignment was satisfactory

+3 indicates that the assignment reflected a deep understanding of the material and conveyed that understanding without resorting to additional length or excessive references.

Of the students completing the assignment, it is expected that 90% will receive a grade of "1".

Collected notes

You are asked to bring a single sheet of paper (a "briefing page") to each class. The page should include your observations on the reading and any questions that you want to ask in class or comments that you want to make. Please be sure that your name is on the sheet. Notes will be randomly collected with a probability such that there will be 4 notes collection events during the semester.

This exercise is based on my real-world experience of having to go to countless leadership meetings with notes about what I would present if I was called upon, as well as specific topics that I knew needed to be raised in the meeting.

Please note:

- **Neither the instructor nor the staff know in advance if notes will be collected on any given day!**
- **Collected notes will not be returned, so be sure you retain a copy!**
- **If collected, it will be graded using the 0-3 scale above.**

Don't go overboard when you are writing your notes! Be strategic. A few bullet points is all you need.

Group Assignments — The Editorial Cartoon and the Short-Form Video

There are two group assignments. All members of the group will receive the same grade.

Final Exam — The Poster Session

During exam week we will have a scheduled "exam" that will be a poster session. There will be two sections, each 1 hour long with 15 minutes between. You are expected to come for both sections.

You have two deliverables:

1. Your poster — Your poster may be any size, but you must print it on paper and bring it to class so that we can affix it to a wall with tape. (If you mount it on posterboard, please bring an easel.)
2. Your 1-page briefing paper. This paper can contain any information you want — additional information, references, pithy quotes, an action plan ... it's up to you.

When you come to class, please bring five copies of your poster printed on 8.5x11" paper with your 1-page briefing paper printed on the reverse side. Be sure your name is on both sides of the paper. Each staff member will take a copy of your paper. You should also upload the poster and the briefing paper to canvas.

Late Assignments

Late assignments will not be accepted without prior arrangement or a waiver in cases of extenuating circumstances.

Citation Practices

Everyone taking this course is working toward a position of public service and trust. Consequently, academic integrity and a solid ethical grounding are vital. It must be shown in this course.

The subject matter of this course is designed to spark discussion, and you are encouraged to talk about everything, including assignments, with your classmates. However, individual work must be done by the individual who takes credit for the work, and use of ideas imported from elsewhere must give credit to the source of the idea. This includes using text written by a generative AI system. You are expected to use these tools, but you must credit their use.

In you writing, you must cite your sources *where they are used*, rather than providing a list of "references" at the end of your document. At minimum, a citation must include the title, author, date, and publication of the reference; **a bare URL is not a sufficient citation and will be ignored.**

Students must be familiar with and must observe Kennedy School and Harvard University rules regarding the citation of sources. Including material from others in the assignments without appropriate quotation marks and citations is regarded, as a matter of School and University policy, as a serious violation of academic and professional standards and can lead to a failing grade in the course, failure to graduate, and even expulsion from the University.

Collaborative Work

Several assignments in this course are collaborative assignments in which all members of a group will receive the same grade for the assignment. **If you feel that you are not being allowed to participate in a group assignment, or if you feel that you have a group member who is not participating,** you should first schedule a group meeting to discuss how you are collaborating as a group and ways for improving the group dynamics. If that meeting does not resolve the situation, you may meet with any member of the course staff either individual or with the entire group.

"You"

In some assignments you will be asked to write about "something that happened to you." If you are unable to write about such an experience in the first person, you are welcome to write about an experience that happened to you or to another person using the *third person*, provided that you have personal knowledge of the event and did not simply read about

Writing Support

HKS has many resources for writing policy memos. Here you can find a memo database, memo writing guidance, and examples of memos from U.S. and international policy practitioners.

https://policymemos.hks.harvard.edu/

https://projects.iq.harvard.edu/files/hks-communications-program/files/lb_how_to_write_pol_mem_9_08_17.pdf

There are also writing consultants available through HKS who can assist in reviewing your policy memos.

https://www.hks.harvard.edu/more/about/leadership-administration/academic-deansoffice/communications-program/consulting#details-appointments

Class Participation

Please review the HKS General Regulations and Standards for the 2025-2026 school year.

In addition to those regulations and standards, please note the following below.

Attendance

You are expected to attend all classes in person. Class will start promptly. If you are late, please enter the room and quietly take your assigned seat.

If you know that you will be unable to attend a specific class, please make arrangements in advance with the course staff.

Note cards

Before each class we will place a note card at each student's seat. You may use this card to write down anything that you wish — doodles, comments, questions or complaints. At the end of class, you can take the card with you or leave it for the teaching staff. You may leave the card unsigned or signed.

Participation – In Class

The working assumption in this class is that we are a community of learners, and that we all have experiences and knowledge that is relevant to the topic and worth sharing.

Given the realities of a large class meeting for 2 hours and 15 minutes once a week, I ask:

1. Please limit yourself to a single question or comment during for each class so that every person in the class can participate.
2. If you are concerned about something that happens in class, please either 1) email me or another member of the class staff, or 2) submit a comment using the anonymous feedback box on Canvas, or 3) write your comment on a notecard and leave it for the class staff when you leave.

Good contributions include:

1. Clear, sound, rigorous, insightful analyses.
2. Comments that thoughtfully challenge conventional or politically safe positions.
3. Realistic recommendations for action.
4. Constructive critiques of others' contributions and impact on the thinking of others.
5. Questions that no one else is willing to ask but that open up productive paths of inquiry.

Don't be afraid to ask a question if you don't know or understand something — if you are confused about something or think that you should know something, but you don't, it's likely that at least three other students are in the same position.

Warm Calling. Please let me know if you would like to be called on to present a personal experience or spend a few minutes presenting a topic in class.

Participation – Online

To understand cybersecurity you must be engaged, asking questions of the material, the practices that you observe in the world around you, and yourself. For this reason, a portion of your grade will be determined by your participation in two forums:

Canvas Discussion "In the news." In this forum, students and class staff can post and discuss news articles that involve cybersecurity.

Canvas "Reflect" Discussions. For some weeks we have created canvas "reflection" assignments in which you are assigned to research or reflect on a topic and post what you have written to Canvas. In addition to writing something, you are also assigned to comment on at least two other student reflections.

Anonymous Class Surveys. Prior to the first class and periodically during the semester we will survey they class. Your identity will not be linked to the survey response (they are "anonymous," a term that we will discuss in class), and what you type may be shared with the class, so **please do not enter confidential or identifying information in the survey response fields**.

Ping Pong. We have created a Ping Pong Group for IGA 236. Please give it a try!

Participation – Optional Friday Sessions

In additional to regularly scheduled class meetings and online class forums, I have scheduled an optional Friday session to dive deeply into tech topics and answer your questions. These sessions on Fridays from 3:00-4:15 in Wex-463.

Course Policies

HKS Non-Attribution Rule

"All HKS events are, unless otherwise explicitly stated, not for attribution. This means you can share in a general way what you learned, but not who said what, without expressed permission. We follow this rule to maintain a culture of mutual respect and trust within our community, and to ensure that we can learn from candid discussion about a wide range of perspectives and experiences.

"The non-attribution rule does not supersede the university's Title IX, Non-Discrimination, and Anti-Bullying Policies. If you have a concern about a potential policy violation, please share your concern with the appropriate official at the Kennedy School."

In this classroom, we follow the non-attribution rule, with the exception of the professor, whose comments are on the record.

Use of Technology for Personal Purposes During Scheduled Class Meetings

HKS discourages the use of technology for personal purposes during classes, seminars, or other professional events. We do this to minimize distractions that might interfere with learning, to maintain a culture of mutual respect and trust within our community, and to ensure that we can learn from candid discussion about a wide range of perspectives and experiences.

Repeated uses of technology for unauthorized purposes in the classroom may result in a reduction of your grade.

If you require an accommodation related to technology, please contact the Associate Director of Disability Services or the Disability Accommodations Coordinator. If you need an exception to these rules due to a family emergency or acute care responsibilities, please talk to your instructor.

Use of Technology in IGA 236

- **For Scheduled Class Meetings:** In this classroom, the use of cell phones, laptops, and tablets is not allowed without permission of the instructor.
- **For optional Q&A Discussion Sessions**: In this classroom, we make regular use of cell phones, laptops, and tablets. However, personal use of these technologies is not allowed without permission of the instructor.
- **Classes will be recorded with the HKS Panopto system during the first week**. After the first week, classes will not be recorded without prior notification.

Class Policy on Generative AI

This course follows the *HKS Policy on Student Use of Generative Artificial Intelligence (AI) for Coursework*. Additionally, this syllabus uses the *Modified AI Traffic Light* model: 🤖 (robot) indicates an assignment for which AI can be used without reservation; 💝 (heart with a yellow ribbon) indicates an assignment in which AI should be used cautiously, and indicated in any materials you hand in. ❤️ (heart) indicates an assignment for which AI should not be used.

Accessibility & Accommodations for Student Learning

Harvard University values inclusive excellence and providing equal educational opportunities for all students. Our goal is to remove barriers for disabled students related to inaccessible elements of instruction or design in this course. If reasonable accommodations are necessary to provide access, please contact the local disability coordinator, Melissa Wojciechowski St. John (melissa_wojciechowski@hks.harvard.edu). She is the Senior Director of Student Services in the HKS Office of Student Services. Accommodations do not alter fundamental requirements of the course and are not retroactive. Students should request accommodations as early as possible, since they may take time to implement. Students should notify Melissa at any time during the semester if adjustments to their communicated accommodation plan are needed.

Student Support Services

Any students experiencing difficulties around an academic, personal, or mental health issue are encouraged to connect with Jimmy Kane, Senior Associate Director of Student Support Services. Jimmy's role is to support students and connect them to resources/individuals so they can continue being successful. He will also provide outreach and support to students when someone in the HKS community has expressed a concern for them.

If students are experiencing any distress and would like to connect with a counselor over the phone, in the evenings, late at night or on the weekends, students are strongly urged to call 617-495-2042 to speak with a CAMHS Cares Counselor.

Readings and Other Materials

There are two kinds three kinds of readings in this class: required readings from the textbook, other required readings, and optional readings.

Students are expected to have read the required readings before class, as the first part of each class will be spent discussing the readings.

Required readings from the textbook

❤️ You should read the text of the book, rather than using AI to summarize the readings.

Our textbook for this course is *Cybersecurity In Context* (CIC), Hoofnagle and Richard, 2024

This text was written by Chris Hoofnagle, a professor of law at University of California, Berkeley, and Golden Richard, a professor of digital forensics at Louisiana State University. This book is the best single text on cybersecurity policy today --- if you can find a better one, please let me know.

We are using a textbook this year because cybersecurity policy is increasingly a comprehensive body of knowledge, and the easiest, most straightforward way of understanding that is to have it in a single book. This book presents technology, theory, case studies, and it does so with a clear voice.

Information for purchasing the textbook (including a discount code) can be found at https://cybersecurityincontext.com/#order

Additional required readings:

Because it is concise, *CIC* misses a few areas. Therefore, we will be supplementing it with readings about:

- Specific case studies
- Supply chain risk management
- Quantum Computing (Hoofnagle and I wrote the book *Law and Policy for the Quantum Age*, which you can download for free from the link)
- Artificial Intelligence
- Digital forensics

These additional required materials will be available through links on Canvas.

Optional Weekly Readings

Optional readings for each week can be found here.

In addition, please see below for recommended supplementary m

Supplementary Materials

Students who wish to go deeper may with to follow:

Podcasts

🤖 Cybersecurity Today with host Jim Love (apple)

Books and Audio Books

🤖 Crypto, Steven Levy, 2001

🤖 This Is How They Tell Me the World Ends: The Cyberweapons Arms Race, Nicole Perlroth, 2021

🤖 Fancy Bear Goes Phishing: The Dark History of the Information Age, in Five Extraordinary Hacks', Scott J. Shapiro, 2023

Weekly cybersecurity e-mail newsletters:

🤖 Wall Street Journal Cybersecurity newsletter: https://www.wsj.com/pro/cybersecurity/newsletters

🤖 *Politico* Weekly Cybersecurity newsletter: https://www.politico.com/newsletters/weekly-cybersecurity

Other resources for current cybersecurity news:

🤖 Wired Security: https://www.wired.com/category/security/

🤖 The Register Security: https://www.theregister.com/security/

🤖 Bleeping Computer: https://www.bleepingcomputer.com/

🤖 Dark Reading: https://www.darkreading.com/

🤖 Cyberscoop: https://cyberscoop.com/

Students without a technical background may find these resources useful:

🤖 Brian W. Kernighan, Understanding the Digital World: What You Need to Know about Computers, the Internet, Privacy, and Security, Princeton University Press, 2017.

🤖 Khan Academy, "Introducing the Internet": https://www.khanacademy.org/computing/computers-and-internet/xcae6f4a7ff015e7d:the-internet

🤖 Rus Shuler, How Does the Internet Work? https://web.stanford.edu/class/msande91si/www-spr04/readings/week1/InternetWhitepaper.htm

🤖 NICCS, A Glossary of Common Cybersecurity Terminology: https://niccs.us-cert.gov/glossary

Detailed Schedule of Class Meetings, Readings, Debates and Assignments

Readings and assignments are subject to change; please follow Canvas for announcements.

Jan 22/23 — Course Preview

❤️ Be sure to fill out the IGA 236 Spring 2026 survey and the SA-6 survey before Jan 26!

Jan 26 & 28 – No textbook for the first week

Jan 26 - Threat modeling and cybersecurity

We will open the class with a discussion of the so-called *CIA Triad* of computer security — the goals of confidentiality*, integrity, and availability*. *Policies* describe in more detail the aspects of these goals that we want to achieve. *Procedures* describe how we go about implementing those policies.

We will then look at threats to CIA, and use that to open our discussion of *threat modeling*—how do we anticipate likely threats to our cybersecurity goals?

As part of our opening discussion, we will focus on the data breach of the credit bureau and data broker Equifax, reported in September 2017, in which personal information from 146 million US persons (about 44% of the population) was reportedly compromised.

Required Readings (~ 1 hour)

❤️ Bruce Schneier, "Inside the Twisted Mind of a Security Professional," *Wired,* Mar 2003. https://www.wired.com/2008/03/securitymatters-0320/

❤️ Gregory Conti, USMA, "Embracing the Kobayashi Maru: Why You Should Teach Your Students to Cheat," IEEE Security and Privacy, July/August 2011

❤️Zack Whittaker, "Equifax Breach Was 'Entirely Preventable' Had It Used Basic Security Measures, Says House Report." TechCrunch, Dec 2018. https://techcrunch.com/2018/12/10/equifax-breach-preventable-house-oversight-report/

Questions for class:

💝 What is your definition of "cybersecurity?"

💝 What is a data center?

💝 Have you ever been the victim of a cybersecurity incident?

💝 What's the difference between a *cybersecurity incident* and a *cybercrime*?

Jan 28 – Privacy and Technology

In this class, we will discuss our notion of privacy, how it interacts with cybersecurity, and preview the important world of privacy enhancing technologies.

Questions to contemplate:

- What's the difference between *privacy* and *confidentiality?*
- Why is privacy not part of the CIA triad?
- Is privacy the wrong word?

Required Readings (~ 1 hour of work)

❤️Stuart A. Thompson and Charlie Warsel, "Twelve Million Phones, One Dataset, Zero Privacy," New York Times, Dec 2019. https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html

❤️ https://en.wikipedia.org/wiki/Information_security#CIA_triad

🤖 "Privacy Enhancing Technologies," The Royal Society. https://royalsociety.org/news-resources/projects/privacy-enhancing-technologies/ Watch the video and browse the 112 page report.

Feb 2 & 4 - CIC 1, “What is Cybersecurity?” (55p)

Feb 2 - Actors, Terrain, and History

❤️ *Required Reading — CIC Chapter 1, “What is Cybersecurity”*

With this class we are starting the book *Cybersecurity in Context*. In this class we dissect the arguments and taxonomies in the first chapter and decide if we agree with them.

Feb 4 - Cryptography

This class will present the basics of encryption, covering hash functions, symmetric encryption, asymmetric encryption, secrecy, digital signatures, and key exchange mechanisms (KEMs).

Required Reading

❤️Understanding Patches and Software Updates,” CISA, 23 Feb 2023. https://www.cisa.gov/news-events/news/understanding-patches-and-software-updates

❤️ An Introduction to Cryptography, Chapter 1, PGP Corporation, 2002. Although dated, this is well-written and kind of fun.

Feb 6 – AMA on Cryptography

Questions on cryptography? Bring them to the optional session on Friday and we’ll work them through.

Feb 9 & 11 - CIC 2, “Technology Basics and Attribution” (pp. 60-85; 24p)

For the second week we will drill down on Internet technology, just so everyone has a solid technical base. The key topic this week is identification: how are things identified, who assigns the identifiers, how they are proven or “proofed,” and how they can be subverted.

Feb 9 – Identifying Machine

We will discuss ways of identifying machines, including serial numbers, MAC (media access control) addresses, IP addresses, the difference between IPv4 and IPv6, WiFi SSIDs, the Domain Name System (DNS), Autonomous System Numbers (ASNs), and TLS certificates.

Feb 11 – Identifying People

We will discuss ways of identifying people, including names, email addresses, certificates, hardware tokens and biometrics, and forensic methods.

Required Reading –

❤️ *An Introduction to Biometrics, International Organization for Migration (IOM), UN MIGRATION, 2023. https://publications.iom.int/system/files/pdf/pub2023-073-r-introduction-to-biometrics.pdf*

🤖 Patergianakis, Antonios, and Konstantinos Limniotis. 2022. "Privacy Issues in Stylometric Methods" *Cryptography* 6, no. 2: 17. https://doi.org/10.3390/cryptography6020017

Feb 18 - CIC 2 Cont., “Technology Basics and Attribution” (pp. 86-108; 22p)

Feb18– Anonymity

Now that we understand how identity is determined by second and third parties, we’ll explore ways of shielding identity to avoid attribution, and we will explore how effective they are.

❤️*Required Watching*

“Shining Light on Internet-based Crimes Against Children,” Brian Levine, USENIX Security ’19. https://www.usenix.org/conference/usenixsecurity19/presentation/levine

Feb 23 & 25 - CIC 3, “Economics and the Human Factor” (30p)

Internet security is fundamentally about technology, but economic considerations and human factors provide the framework in which the technology operates. Economics frequently determines what systems get deployed, how they are defended, and how much effort is spent exploiting them. Whether or not those systems can be compromised in practice depends not just on the technology, but on the humans behind the keyboard—those who designed and deployed those systems, those who are using them, and those who are attacking.

Feb 23 – Human Factors and Phishing

Required Reading — CIC Chapter 3

Additional Required Reading

Adam Engst, “An Annotated Field Guide to Identifying Phish,” TidBITS, Jan 2023. https://tidbits.com/2023/01/16/an-annotated-field-guide-to-identifying-phish/

“Batman Hacked My Password: A Subtitle-Based Analysis of Password Depiction in Movies,” Maike M. Raphael, Leibniz University Hannover; Aikaterini Kanta, University of Portsmouth; Rico Seebonn and Markus Dürmuth, Leibniz University Hannover; Camille Cobb, University of Illinois Urbana-Champaign, SOUPS 2024, https://www.usenix.org/conference/soups2024/presentation/raphael (Read the paper or watch the video)

“Knowledge and Capabilities that Non-Expert Users Bring to Phishing Detection,” Rick Wash, Norbert Nthala, and Emilee Rader, SOUPS 2021 https://www.usenix.org/conference/soups2021/presentation/wash (Read the paper or watch the video)

Feb 25 – The economics of cybersecurity – costs to organizations

We will discuss human factors and economics from the point of view of organizations.

Additional Required Reading

Ross Anderson, “Why Information Security Is Hard: An Economic Perspective,” *17th Annual Computer Security Applications Conference,* Dec 2001. https://www.acsac.org/2001/papers/110.pdf

Mar 2 & 4 - CIC 4, “The Military and Intelligence Communities” (56p)

Mar 2 – — Patches and Software Updates

Required Reading — CIC Chapter 4

Mar 4 – VEP Debate

Additional Required Reading (Sorry!)

Josh Kenway and Michael Garcia, “To Patch or Not to Patch: Improving the US Vulnerabilities Equities Process,” Third Way, 1 Jun 2021. https://www.thirdway.org/memo/to-patch-or-not-to-patch-improving-the-us-vulnerabilities-equities-process

GCHQ, “The Equities Process,” 19 Nov 2018. https://www.gchq.gov.uk/information/equities-process

US Government, “Vulnerabilities Equities Policy and Process for the United States Government,” Nov 2017. https://trumpwhitehouse.archives.gov/sites/whitehouse.gov/files/images/External%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF

Mar 9 & 11 - CIC 5, “Cybersecurity Theory” (52p)

Mar 9 - Theory

Required Reading — CIC Chapter 5

Mar 11 – Practice — CIA for Data and Metadata

Canvas Reflect: Your Security Plan

Review the EFF’s guide “Your Security Plan” and other modules in the Surveillance Self-Defense Guide that you find relevant. Policymakers invariably make decisions that are informed by their own experience. How does the threat model of individuals differ from those of organizations and countries, and how are they similar? Write your reflections on Canvas, and respond to at least two of your classmates.

Additional Reading

Your Security Plan EFF Surveillance Self-Defense, 2023. https://ssd.eff.org/module/your-security-plan

Mar 23 & 25 - CIC 6, “Consumer Protection Law” (32p)

Mar 23 – Surveillance Capitalism

Required Reading — CIC Chapter 6

Mar 25 – Who Gets Access to Your Data?

Required Reading

Phillip Rogaway, “The Moral Character of Cryptographic Work,” Essay to accompany the 2015 ACR Distinguished Lecture. Cryptology ePrint Archive, Report 2015/1162. 2015 https://web.cs.ucdavis.edu/~rogaway/papers/moral.html

Mar 30 & Apr 1- CIC 7, “Criminal Law” (52p)

Cybercrime is a worldwide multibillion-dollar business. It comprises a wide variety of tactics, from stealing financial credentials and conducting credit card fraud to data theft and extortion. We will discuss the evolution of different models of financially motivated cybercrime over the 15 years through the lens of two case studies:

1. The case of Russian hackers Maksim Yakubets and Igor Turashev, who were indicted by the Department of Justice in 2019 for distributing the Bugat, or Dridex, malware and using it to steal hundreds of millions of dollars.
2. The hacking effort by Jon Chang Hyok, Kim Il, and Park Jin Hyok, of North Korea, who hacked into multiple systems from 2009 through 2020 according to the indictment, including the hack on Sony Pictures in retaliation for the creation and intended release of the movie “The Interview.”

Mar 30 – Phishing, DDoS, Ransomware, BGP Attacks, Cyber Insurance policy

Required Reading — CIC Chapter 7

Apr 1 – Virtual NOC

Additional Required Reading

Jareth, “To pay or not to pay ransomware: A cost-benefit analysis of paying the ransom, Emisoft blog, 20 Aug 2019. https://blog.emsisoft.com/en/33686/to-pay-or-not-to-pay-ransomware-a-cost-benefit-analysis-ofpaying-the-ransom/

United States v. Miksim Viktorovich Yakubets and Igor Turashev, “Criminal Complaint,” Nov 2019. https://www.justice.gov/opa/press-release/file/1223586/download

United States v. Jon Chang Hyok, Kim Il, and Park Jin Hyok, “Indictment, Jan 2020. https://www.justice.gov/opa/press-release/file/1367701/download

Apr 6 & 8 - CIC 8, “Critical Infrastructure” (34p)

Apr 6 –Resilience

Required Reading — CIC Chapter 8

Apr 8 – AI as Critical Infrastructure

“Disrupting malicious uses of AI by state-affiliated threat actors,” OpenAI, 14 Feb 2024. https://openai.com/index/disrupting-malicious-uses-of-ai-by-state-affiliated-threat-actors/

Giovanni Apruzzese et al, “Real Attackers Don't Compute Gradients”: Bridging the Gap Between Adversarial ML Research and Practice”, *2023 IEEE Conference on Secure and Trustworthy Machine Learning (SaTML), Year: 2023, Pages: 339-364 DOI Bookmark: 10.1109/SaTML54575.2023.00031*
https://www.computer.org/csdl/proceedings-article/satml/2023/629900a339/1NCHHH6qvS0
https://arxiv.org/abs/2212.14315

“The Framework Convention on Artificial Intelligence,” Council of Europe. https://www.coe.int/en/web/artificial-intelligence/the-framework-convention-on-artificial-intelligence

Apr 13 & 15 - CIC 9, Intellectual Property Rights” (26p)

Apr 13 – Intellectual Property

Required Reading — CIC Chapter 9

Apr 15 – Web Scraping and Open Source Intelligence

Chris Rasmussen, How the Intelligence Community Has Held Back Open-Source Intelligence, and How It Needs to Change, Studies in Intelligence, Vol 68, No. 2.

Călin Ioan JULAN and Mihai TOGAN, Methodologies for Retrieving and Processing Information from Open Sources (OSINT), Journal of Military Technology, Vol 6, No. 1, June 2023.

Carahsoft, OSINT Buyer’s Guide for Government, 2024. https://static.carahsoft.com/concrete/files/2717/4250/0619/Carahsoft_OSINT_Buyers_Guide_2024_-_Updated_3.7.25_1.pdf

Apr 20 & 22 - CIC 10, “The Private Sector” (50p)

April 20 – Insider Threat

Required Reading — CIC Chapter 10

Optional

Center for Development of Security Excellence, Defense Counterintelligence and Security Agency, Insider Threat Awareness Training. https://securityawareness.dcsa.mil/itawareness/index.htm

Apr 22 - Supply Chain Security

Protecting Critical Supply Chains: Building a Resilient Ecosystem, US Director of National Intelligence, (2024). https://www.dni.gov/files/NCSC/documents/supplychain/Building-a-Resilient-Ecosystem.pdf

US Department of Energy, Supply Chain Cybersecurity Principles (2024). https://www.energy.gov/sites/default/files/2024-06/DOE%20Supply%20Chain%20Cyber%20Princples%20June%202024.pdf

Security Scorecard, 2025 Supply Chain Cybersecurity Trends. https://securityscorecard.com/wp-content/uploads/2025/06/2025-Supply-Chain-Cybersecurity-Trends.pdf

Apr 27 & 29 - CIC 11, “Cybersecurity Tussles” (20p)

The book discusses five tussles:

1. Software Liability
2. Technical Computer Security vs. Cybersecurity, in which alternatives to invincible security are considered such as criminal law, consumer law and industrial policy.
3. Encryption and Exceptional Access
4. Disinformation and racist speech.

Apr 27 - Tussle 1

TBD

Apr 22 – Tussle 2

TBD

May 4 & 6 - CIC 12, “Cybersecurity Futures” (18p)

May 4 – Quantum Computing

Required Reading

“Securing Information in the Quantum Computing Agen: Managing the Risks to Encryption,” Michael J. D. Vermeer and Evan D. Pett, Rand Corporation, Research Report RR3102, April 9, 2020.

May 6 – Futures 2

TBD

May 11-15 – Final Assessment — Poster and 1-page Briefing Paper

May 11, 12, 13, 14 or 16 –