



Cybersecurity in Context
LEGALST 190.002 / Class 30870
Classroom: 104 Wheeler Hall
TuTh 2:00P-3:29P
Instructor: Chris Hoofnagle
Office Hours: M 1-2, 341 Berkeley Law

Cybersecurity is instrumental to economic activity and human rights alike. But as digital technologies penetrate almost every aspect of human experience, a broad range of social- political-economic-legal-ethical-military and other considerations have come to envelop the cybersecurity landscape.

Cybersecurity in Context (CiC) explores the most important elements that shape the playing field on which cybersecurity problems emerge and are managed. The course will emphasize how ethical, legal, and economic frameworks enable and constrain security technologies and policies. It will introduce some of the most important macro-elements (such as national security considerations and the interests of nation-states) and micro-elements (such as behavioral economic insights into how people understand and interact with security features).

CiC includes a computer major lab component designed to upskill students and expose them to the actual technologies and methods of computer attack, because in order to understand defense, one must be familiar with offense. Students will pledge to not use this knowledge for any illegal or unethical purpose.

There are no prerequisites for this course and it is not necessary to have programming or other advanced computer skills.

Course requirements

- Chris Jay Hoofnagle & Golden G. Richard III, [Cybersecurity in Context](https://www.wiley.com/en-us/Cybersecurity+in+Context%3A+Technology%2C+Policy%2C+and+Law-p-9781394262441) (https://www.wiley.com/en-us/Cybersecurity+in+Context%3A+Technology%2C+Policy%2C+and+Law-p-9781394262441) (Wiley 2024). There is a 20% discount if you use the code ENG20 on Wiley.com.
 - Chapter 1---our first reading---is available online free here:
https://media.wiley.com/product_data/excerpt/42/13942624/1394262442-5.pdf (https://media.wiley.com/product_data/excerpt/42/13942624/1394262442-5.pdf)
- A PC or a Mac (the labs will not work with Chromebooks or iPads)
 - The STEP program is available to students who need devices <https://studenttech.berkeley.edu/devicelending> (https://studenttech.berkeley.edu/devicelending).

Before the course: prepare your computer

Please bring your computer to class every day because we will be doing computer labs! These are designed for students with no programming experience whatsoever. Yet, we will do some advanced topics, such as malware analysis.

To prepare for the labs, please visit this page <https://cybersecurityincontext.com/labs/> (https://cybersecurityincontext.com/labs/) (password is: context) and follow the instructions for downloading the Virtual Machine software (known as a "Hypervisor", VMWare's Workstation for PCs or Fusion for Mac) the Virtual Machine for this course, and the labs. The Virtual Machine environment will allow us to do labs without altering your own computer. Please note---the environment is very large (about 50GB) and so it may take hours to download. You will not have time to do this the day of class.

Course schedule

Day	Date	Class Topic	Reading
Part 1: Cybersecurity Fundamentals			

Th	29-Aug	Introduction: what is cybersecurity?	Chapter 1. Note: if you are course shopping, you can download chapter 1 from Wiley's website before buying the textbook Please prepare your computer for the labs (see instructions above). This will take about 15 minutes of work, but the download may take a few hours.
Tu	3-Sep	What is cybersecurity continued	Please read the Lab 1 instructions (https://bcourses.berkeley.edu/courses/1537157/files/89343526?wrap=1) , we will do the lab in class.
Th	5-Sep	Technology basics; the Attribution Problem	Chapter 2
Tu	10-Sep	Tech continued	Please read the Lab 2 instructions
Th	12-Sep	Class Cancelled	
Part 2: Fundamental Social Factors in Cybersecurity			
Tu	17-Sep	The economics and psychology of cybersecurity	Chapter 3
Th	19-Sep	Economics continued	Please read the Lab 3 instructions
Fr	20-Sep	Assignment 1 Due (https://bcourses.berkeley.edu/courses/1537157/assignments/8796006)	
Tu	24-Sep	The Military and Intelligence Community	Chapter 4
Th	26-Sep	Military continued	Please read the Lab 4 instructions
Fr	27-Sep	Optional Makeup: Cybersecurity and the Clean Energy Transition	Register here (https://www.eventbrite.com/e/cybersecurity-and-the-clean-energy-transition-tickets-965274480957)
Tu	1-Oct	Cybersecurity Theory	Chapter 5
Th	3-Oct	Theory continued	Please read the Lab 5 instructions
Tu	8-Oct	Class Cancelled	
Th	10-Oct	Class Cancelled	
Part 3: Substantive Cybersecurity Law and Policy			
Tu	15-Oct	Consumer law cybersecurity	Chapter 6
Th	17-Oct	Consumer law continued	Please read the Lab 6 instructions
Tu	22-Oct	Criminal law cybersecurity	Chapter 7
Th	24-Oct	Criminal continued	Please read the Lab 7 instructions

Fr	25-Oct	Assignment 2 due (https://bcourses.berkeley.edu/courses/1537157/assignments/8796008)	
Tu	29-Oct	Critical Infrastructure cybersecurity	Chapter 8
Th	31-Oct	CI continued	Please read the Lab 8 instructions
Tu	5-Nov	Intellectual Property Law cybersecurity	Chapter 9
Th	7-Nov	Sextortion and harassment	Please read the Lab 9 instructions
Tu	12-Nov	Private Sector Cybersecurity	Chapter 10
Th	14-Nov	Private Sector continued	
Tu	19-Nov	Private Sector continued	Please read the Lab 10 instructions
Part 4: Cybersecurity Today and Tomorrow			
Th	21-Nov	Cybersecurity Tussles	Chapter 11
Tu	26-Nov	Final Presentations	
Th	3-Dec	Cybersecurity Futures	Chapter 12
Tu	5-Dec	Final Presentations	
We	6-Dec	Final paper due (https://bcourses.berkeley.edu/courses/1537157/assignments/8796022)	

Assessment

Three, relatively-short memos will form the basis of most assessment (80%). The remaining 20% will reflect class participation, lab completion, and attendance.

Attendance and Class Policy

Attendance is required. However, if you are feeling ill, all illness-related absences will be excused. Simply email me. Get lecture notes from a colleague.

A note on devices. In July 2023, Unesco recommended that smartphones be banned in schools because many studies now show that devices reduce educational performance. Please only use your devices for class-related activity. The best strategy is probably to take notes with paper and then refactor them on your computer.

Optional Materials: Tech Literacy

This course will have a substantial, introductory technology component. Yet if you want to brush up on your skills, please consider:

- [LinkedIn Learning](https://hr.berkeley.edu/linkedin-learning) (<https://hr.berkeley.edu/linkedin-learning>) (formerly Lynda.com) is available to the entire Berkeley community and it has good quality online, go-at-your-own-pace courses in the Bash command line, in cybersecurity management, the technical domains of cybersecurity (computer networking, endpoint, application, cloud, operating system), security testing, penetration testing, machine learning, python, statistics, and statistical management software, such as R.
- [D-Lab](https://dlab.berkeley.edu/) (<https://dlab.berkeley.edu/>) is another valuable resource. D-Lab regularly teaches bootcamps in technical fields such as Bash, R, and Python. Courses are free but they fill quickly.



APM-015 Part II statement

This course will deal with material concerning current events, historical events, absurd hypotheticals, and exploration of government actions and their possible consequences. Class discussion will feature such material.

Learning outcomes

- Understand the elements that define “cybersecurity”
- Understand the legal, social, and political frameworks that affect cybersecurity
- Identify and define challenges to achieving cybersecurity
- Identify and explain social, legal, political, and economic impediments to cybersecurity
- Suggest approaches to maintain a reasonable state of cybersecurity and to address breaches effectively, ethically, and according to law
- Identify main tradeoffs between different cybersecurity-related interests (e.g., between economics and security levels; between law enforcement and civil liberties; between private interests and public interests)
- Learn the basics of computer network exploitation and attack







Going deeper: excellent resources

- Bruce Schneier's [CryptoGram](https://www.schneier.com/crypto-gram/)  [\(https://www.schneier.com/crypto-gram/\)](https://www.schneier.com/crypto-gram/)
- [LawFare](https://www.lawfaremedia.org/)  [\(https://www.lawfaremedia.org/\)](https://www.lawfaremedia.org/)
-  [\(https://www.lawfaremedia.org/\)](https://www.lawfaremedia.org/) [Krebs on Security](https://www.krebsonsecurity.com/)  [\(https://www.krebsonsecurity.com/\)](https://www.krebsonsecurity.com/)

Careers in Cybersecurity

Are you interested in a career in cybersecurity? See our [FAQ \(https://cybears.berkeley.edu/\)](https://cybears.berkeley.edu/) on cybersecurity resources at Cal.

Course Summary:

Date	Details	Due
Fri Sep 20, 2024	 Assignment 1: Country Cyber Assessment (https://bcourses.berkeley.edu/courses/1537157/assignments/8796006)	due by 11:59pm
Sat Sep 28, 2024	 Academic Integrity Assignment (Fall 2024) (https://bcourses.berkeley.edu/courses/1537157/assignments/8807801) (Academic Integrity Assignment (Fall 2024))	due by 12:59am
	 Academic Integrity Assignment (Fall 2024) (https://bcourses.berkeley.edu/courses/1537157/assignments/8807801)	due by 12:59am
Tue Oct 1, 2024	 Extra Credit Opportunity --- Cyber Intelligence: The NSA View and Critiques (https://bcourses.berkeley.edu/courses/1537157/assignments/8814704)	due by 11:59pm
Fri Oct 25, 2024	 Assignment 2: Theory (https://bcourses.berkeley.edu/courses/1537157/assignments/8796008)	due by 11:59pm
Fri Dec 6, 2024	 Assignment 3: Options Memo (https://bcourses.berkeley.edu/courses/1537157/assignments/8796022)	due by 11:59pm