# The Cyber World — Fall 2021
# The Global Master of Arts Program

Laurin Weissinger

Laurin.weissinger@tufts.edu

**Version 1.2, September 2021**

## Contents

# 1 Course Objectives

This course is meant to teach students about the intersection of networked digital technologies with society, the economy, the international system, as well as policy and governance. The key objectives include: giving some key insights into how technology works, increasing students' skills in understanding and addressing technology issues, and helping students to situate technology in its wider context. The course will start with introducing key topics and issues on a more theoretical level, and dive into four case studies and an outlook session during the online period.

# 2 Contact & Office Hours

Due to the fact that we will be online and spread across the globe, please email me at `laurin.weissinger@tufts.edu` or use the Fletcher office hour booking tool to schedule office hours. My "official" office hours will be on Tuesday (please agree on a time nevertheless, due to the hybrid nature of teaching this year!). I will make myself available outside those time slots by appointment.

# 3 Accommodations

As a hybrid online/offline class, the Cyber World class is relatively flexible in terms of accommodations. Should you need any extension or accommodation due to COVID or any other reason, please contact me. Some extensions or accommodations might require me to liaise with GMAP staff. Thus, if possible, I appreciate receiving notice early. However, we all understand that this is not always possible.

# 4 Residency Period

The lectures and discussions during the residency period will introduce students to the relevant, underpinning technical issues. These sessions provide an overview and a reference for students before diving into specific cases that will cut across multiple layers and issues. Each session will require some preparation, and be broken up into a lecture, followed by class discussion. As technical issues are extremely relevant to this course, explanations of how things work "on the ground" will be part of these lectures.
Some of the material will be new to some of you but together with the pre-course reading, you will learn about how computers work and become familiar with certain terms and ideas before we are diving into policy questions.

### Pre-course Reading

**Kernighan, Brian (2017) Understanding the Digital World. Princeton University Press.**

**Please do some reading before watching the initial video lecture on Canvas.**

*Note: The substance of the book might be new to you. Do not worry about it, the book is assigned to provide an overview and we will revisit key subjects.*

Benkler, Yochai (2001) **The battle over the institutional ecosystem in the digital environment**. Commun. ACM, vol. 44, no. 2, 84—90.
`https://cacm.acm.org/magazines/2001/2/7460-the-battle-over-the-institutional-ecosystem-in-the-digital-environment/fulltext`

Zittrain, Jonathan (2014) **No Barack Obama Isn't Handing Control of the Internet Over to China New Republic.** New Republic. March 24, 2014.
`https://newrepublic.com/article/117093/us-withdraws-icann-why-its-no-big-deal`

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

## 4.1 Lecture One: Internet and Digital Infrastructure — Prerecorded. Please watch after the reading but before the residency.

This lecture will provide an introduction into "the basics": how do computers work? How does the internet work? What are the key aspects of infrastructure and the key technical debates that policy makers should be aware of? Specifically, we will discuss the following:

1. History: How did this all start?
2. Physical Infrastructure: undersea cables, copper, and glass fiber
3. Equipment: routers, switches, satellites
4. The key layers of what makes the internet: addressing, routing, naming
5. Why does technology matter to policy makers?

**Further Reading (optional):**

Partridge, Derek (2011) **The Seductive Computer. Why IT Systems Always Fail.** Springer, New York.

DeNardis, Laura (2015) **The Internet Design Tension between Surveillance and Security.** IEEE Annals of the History of Computing 37, no. 2 (April 2015): 72–83.

### 4.2 Lecture Two: Political Economy and Digital Equity — August 11, 12:20-1:40pm ET

In 2020, the seven most valuable companies (by market cap) are all IT and technology firms, and the six biggest are US-based. These digital behemoths shape our lives but the economic impacts of computer technologies do not benefit everyone equally. Specifically, we will discuss the following:

1. The impact of connected technology on humans and the economy
2. How companies make money in this space
3. Who wins and who loses in this connected world

**Further Reading (optional):**

Graham, Mark (2011). **Time Machines and Virtual Portals: The Spatialities of the Digital Divide.** Progress in Development Studies. 11 (3): 211–227.

James, Jeffrey (2005). **The global digital divide in the Internet: developed countries constructs and Third World realities.** Journal of Information Science. 31 (2): 114–23.

Zuboff, Shoshana (2019) **The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power.** New York: PublicAffairs.

MacKinnon, Rebecca (2012) **Consent of the Networked: The Worldwide Struggle For Internet Freedom.** Hachette, New York.

### 4.3 Lecture Three: Global Internet Governance — August 12, 10:40-12 noon ET

As lecture one and two established, the internet, computer technology, and the economy built around it are complex themselves and bring about equally complex policy and governance debates. Who is in charge of the global internet, and who ultimately calls the shots? Specifically, we will discuss the following:

1. The roles of ICANN, IETF, IEEE, and the ITU in technology governance and development
2. The importance of nation states and international organizations in this space
3. International and transnational agreements and contracts
4. Why is the internet hard to govern?

**Further Reading (optional):**

Leiner, Barry et al (2009) **A Brief History of the Internet.** ACM SIGCOMM Computer Communication Review, 39:5 (2009)22-31

DeNardis, Laura (2009) **Protocol Politics: The Globalization of Internet Governance.** The MIT Press, Cambridge.

### 4.4 Lecture Four: Cybersecurity and Cybercrime — August 13, 9:00-10:20am ET

Many key aspects of life are now digital – for example banking, communications, and some government services. Internet voting is already being practiced in some countries. Unsurprisingly, such use cases create the need to address digital security to fight against increasing risks of cybercrime and threats to critical infrastructure. Specifically, we will discuss the following:

1. How digital systems can be attacked (e.g. vulnerabilities, back doors)
2. The CIA Triad (Confidentiality, Integrity, Availability)
3. Cybercriminals and how they operate

**Further Reading (optional):**

Van Eeten et al (2010) **The Role of Internet Service Providers in Botnet Mitigation: An Empirical Analysis Based on Spam Data.** TPRC 2010.

Lusthaus, Jonathan (2018) **Industry of Anonymity**. Harvard University Press, Cambridge.

### 4.5 Lecture Five: National Security — August 13, 10:40-12:00 noon ET

Considering the economic and societal impact of digital technology, it is unsurprising that states have a variety of critical national security concerns. These concerns include espionage and cyberattacks by foreign actors, but also market dominance, trade policy, taxation, and supply chains. Specifically, we will discuss the following:

1. Cyberattacks, espionage, and how they are handled
2. Infrastructure and supply chains
3. Information Operations
4. Weaponizing technology firms: is this realistic?

**Further Reading (optional):**

Kenneth Geers (2015) **Cyber War in Perspective: Russian Aggression Against Ukraine.** NATO CCD COE Publications, Tallinn 2015.

Commission on Enhancing National Cybersecurity (2016) **Report on Securing and Growing the Digital Economy**

# 5 Online Period: Case Studies

During the online element of the course, each week will deal with one specific area through the lens of a case study. Session one will speak to regulation and national interests, Session two will go into detail when it comes to complexity and cybercrime response, Session three will look into state-sponsored campaigns. Then, Session four will discuss different approaches to digitize the state, and Session five will focus on what the future may hold. Reading for these sessions will be a mix of case-study related materials, and more general texts.

## 5.1 Session One: The Tech Giants? Regulation, Taxes, Surveillance, and Privacy — Fall Term Week 7: October 12-18

Some have portrayed the GDPR and other recent EU actions as an attack on successful US companies, trying to tax foreign firms while being a digital wasteland themselves. Is this a story of different priorities, or an example of indirect punitive action? What about taxing these successful giants, who has the power to deal with them?

**Reading:**

Lauchlan, Stuart (2020) **The digital policy divide between the US and the EU - a bridge too far when Eurocrats collide with the MAGA-mindset?**
`https://diginomica.com/digital-policy-divide-between-us-and-eu-bridge-too-far-when-eurocrats-collide-maga-mindset`

Eichensehr, Kristen (2018) **Digital Switzerlands**
`https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3205368`

Klein, Adam I. (2016) **Decryption Mandates and Global Internet Freedom**
`www.hoover.org/sites/default/files/research/docs/klein_webreadypdf.pdf`

Abelson et al (2015) **Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications**
`https://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf`

## 5.2 Session Two: Communities that fight abuse: The Conficker case — Fall Term Week 8: October 19-25

Profit-driven cybercrime has only increased in volume and damage in recent years. Ransomware, targeted attacks, cyber vandalism but also mistakes, oversights, and unforeseen events put technology owners at risk. A variety of communities, usually a mix of official and private actors, work together to keep the internet secure, applying their specific positions, skills, abilities, and powers. Based on real-world examples, we will explore

how these groups work.

**Reading:**

Conficker Working Group (2010). **Lessons Learned.**
https://www.fbiic.gov/public/2011/jan/conficker_working_group_lessons_learned_17_June_2010_final.pdf

Shin, Seungwon and Gu, Guofei (2010) **Conficker and beyond: a large-scale empirical study.** In Proceedings of the 26th Annual Computer Security Applications Conference (ACSAC '10)
https://doi.org/10.1145/1920261.1920285

## 5.3 Session Three: APT1 and Stuxnet: How states become active in cyberspace — Fall Term Week 9: October 26 – November 1

States project their power in cyberspace and use digital tools to get what they want. Based on real world cases, this session will explore what happens if they do, how they get found out, and what happens after.

**Reading:**

Fireeye Inc. **APT1: Exposing One of China's Cyber Espionage Units**
https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf

Thomas Rid (2011) **Cyber War Will Not Take Place**
https://www.tandfonline.com/doi/pdf/10.1080/01402390.2011.608939

**Further Optional Reading:**

Shackelford, Scott J. and Russell, Scott (2016) **Operationalizing Cybersecurity Due Diligence: A Transatlantic Comparative Case Study**. South Carolina Law Review.
https://ssrn.com/abstract=2714529

## 5.4 Session Four: Digital Society? Comparing Estonia, Germany, and the United States — Fall Term Week 10: November 2-8

Digitization of public services is a key issue in a variety of countries. Estonia was an early starter and remains a key example and benchmark. Germany and the United States, on the other hand, have been slower to digitize, with different policy challenges and concerns driving or limiting their move towards digital civil services.

**Reading:**

Homero Gil de Zúñiga, Aaron Veenstra, Emily Vraga & Dhavan Shah (2010) **Digital Democracy: Reimagining Pathways to Political Participation**. Journal of Information Technology & Politics, 7:1, 36-51.
https://www.tandfonline.com/action/showCitFormats?doi=10.1080%2F19331680903316742

Pickup, Oliver (2018) **Estonia: the world's most advanced digital society?**
https://www.raconteur.net/technology/estonia-digital-society

Schulze, Elizabeth (2019) **How a tiny country bordering Russia became one of the most tech-savvy societies in the world**
https://www.cnbc.com/2019/02/08/how-estonia-became-a-digital-society.html

Brady, Kate (2018) **Germany launches digital strategy to become artificial intelligence leader** DW.de
https://www.dw.com/en/germany-launches-digital-strategy-to-become-artificial-intelligence-leader/a-46298494

**Further Optional Reading:**

Matthew Hindman (2008) **The Myth of Digital Democracy**. Princeton University Press.

## 5.5 Session Five: Outlook: AI, Block Chain, Quantum Computing: what is next, what matters? — Fall Term Week 11: November 9-15

This last session will deal with emerging technologies: what are the key developments at this point in time, what might their impact be in different countries and regions? Will there be a revolution or simply evolution?

**Reading:**

Anderson, Ross (2008) Security Engineering **The Bleeding Edge** (This is from 2008!)
https://www.cl.cam.ac.uk/~rja14/Papers/SEv2-c23.pdf

Schneier, Bruce (2017) **Click Here to Kill Everybody: Security and the Internet of Things**. New York Magazine, Jan 2017.
http://nymag.com/selectall/2017/01/the-internet-of-things-dangerous-future-%20bruce-schneier.html

Popa, Raluca and Zeldovich, Nikolai (2015) **How to Compute With Data You Can't See.** https://spectrum.ieee.org/computing/software/how-to-compute-with-data-you-cant-see

# 6 Assessment:

Please see Canvas for more detailed instructions on how to complete each assignment.

## 6.1 Forum Participation – 20%

There will be discussions every week, please contribute.

**Outcome:** Discussion on the forum, e.g. sharing ideas and relevant articles.

**Deadline:** Throughout. Cut off: December 7th, 2021, 23:59 Pacific Time.

## 6.2 Quizzes – 30%

There will be one short quiz or task per week. This means one after the residency period and one per week during the online period. These quizzes will be short, e.g. asking some quick questions about the session and material. This helps you making sure that you understood the key concepts and issues, and helps me gauging how to proceed, and what topics to revisit.

**Outcome:** Completed Quiz Assignment on Canvas.

**Deadlines:** Specific dates will be announced on Canvas, where you will also submit your answers. You will have 10 days to complete each quiz during the online period and two weeks after the residency.

## 6.3 Briefing Paper about a technology policy issue – 25%

**Going through all the case studies is not required for this piece**, and everything submitted before the online period will be assessed as such. For those of you who prefer to submit after, submission will be open until November 30$^{\text{th}}$.

I am more than happy for you to write about any topic of import that is related to the material (e.g. cases relevant in your countries of origin/residence, recent events, etc.). **Please email me with your title and two-three sentences about your paper before starting your work.**

**Outcome:** Briefing Paper, target length **one** page, 11pt font.

**Deadline:** November 30th, 2021, 23:59 Pacific Time.

## 6.4 Small Group Project: Topic to be confirmed. 25%

The topic will be about an issue that involves technology, society, and policy. It will be topical, current, and multidimensional.

**Last Year's Project: Electronic Voting**
The country of Hyrule wants to use internet voting for their next election. They are a smaller but diverse democratic Nation with relatively few internal divisions. Nevertheless, trust in the election outcome is of utmost

importance. Furthermore, the country is at risk from both Nation State adversaries as well as criminals. Design a high-level plan for the voting system. Think about security risks but also access, costs, etc.

**Outcome**: Exposé, 5-7 pages, including figures and a half-page executive summary, excluding the bibliography. This is an applied, policy-focused brief, not an academic paper!

**Deadline:** December 7th, 2020, 23:59 Pacific Time.

# 7 Links to Optional Reading

**These readings are not required to complete the class successfully!**

This list is for those who plan to do their capstone project on a technology policy topic or are otherwise interested in further reading. This list includes many books.

Partridge, Derek (2011) **The Seductive Computer. Why IT Systems Always Fail.** Springer, New York.
https://www.springer.com/gp/book/9781849964975

DeNardis, Laura (2015) **The Internet Design Tension between Surveillance and Security.** IEEE Annals of the History of Computing 37, no. 2 (April 2015): 72–83.
https://ieeexplore.ieee.org/document/7116471

Graham, Mark (2011). **Time Machines and Virtual Portals: The Spatialities of the Digital Divide.** Progress in Development Studies. 11 (3): 211–227.
https://journals.sagepub.com/doi/10.1177/146499341001100303

James, Jeffrey (2005). **The global digital divide in the Internet: developed countries constructs and Third World realities.** Journal of Information Science. 31 (2): 114–23.
https://journals.sagepub.com/doi/10.1177/0165551505050788

Zuboff, Shoshana (2019) **The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power.** New York: PublicAffairs.
https://www.publicaffairsbooks.com/titles/shoshana-zuboff/the-age-of-surveillance-capitalism/9781610395700/

MacKinnon, Rebecca (2012) **Consent of the Networked: The Worldwide Struggle For Internet Freedom.** Hachette, New York.
https://consentofthenetworked.com/

Leiner, Barry et al (2009) **A Brief History of the Internet.** ACM SIGCOMM Computer Communication Review, 39:5 (2009)22-31
https://www.internetsociety.org/internet/history-internet/brief-history-internet/

DeNardis, Laura (2009) **Protocol Politics: The Globalization of Internet Governance.** The MIT Press, Cambridge.
https://mitpress.mit.edu/books/protocol-politics

Van Eeten et al (2010) **The Role of Internet Service Providers in Botnet Mitigation: An Empirical Analysis Based on Spam Data.** TPRC 2010.
https://www.oecd-ilibrary.org/science-and-technology/the-role-of-internet-

service-providers-in-botnet-mitigation_5km4k7m9n3vj-en

Lusthaus, Jonathan (2018) **Industry of Anonymity**. Harvard University Press, Cambridge.
https://www.hup.harvard.edu/catalog.php?isbn=9780674979413

Kenneth Geers (2015) **Cyber War in Perspective: Russian Aggression Against Ukraine.** NATO CCD COE Publications, Tallinn 2015.
https://ccdcoe.org/library/publications/cyber-war-in-perspective-russian-aggression-against-ukraine/

Commission on Enhancing National Cybersecurity (2016) **Report on Securing and Growing the Digital Economy**
https://archive.org/details/report_digital_economy_2006_librivox
https://obamawhitehouse.archives.gov/sites/default/files/docs/cybersecurity_report.pdf

Shackelford, Scott J. and Russell, Scott (2016) **Operationalizing Cybersecurity Due Diligence: A Transatlantic Comparative Case Study**.
South Carolina Law Review.
https://ssrn.com/abstract=2714529

Matthew Hindman (2008) **The Myth of Digital Democracy**. Princeton University Press.
https://princetonup.degruyter.com/view/title/550238?language=en