CE876 - Information Security Mng. & Eng.

Lecture 1: Introduction

Department of Computer Engineering
Sharif University of Technology
Spring 1400

S4Lab

Acknowledgments: Some of the slides are fully or partially obtained from other sources. A reference is noted on the bottom of each slide to acknowledge the full slide or partial slide content. These slides were initially developed by Seyedeh Atefeh Musavi and Mehdi Kharrazi.

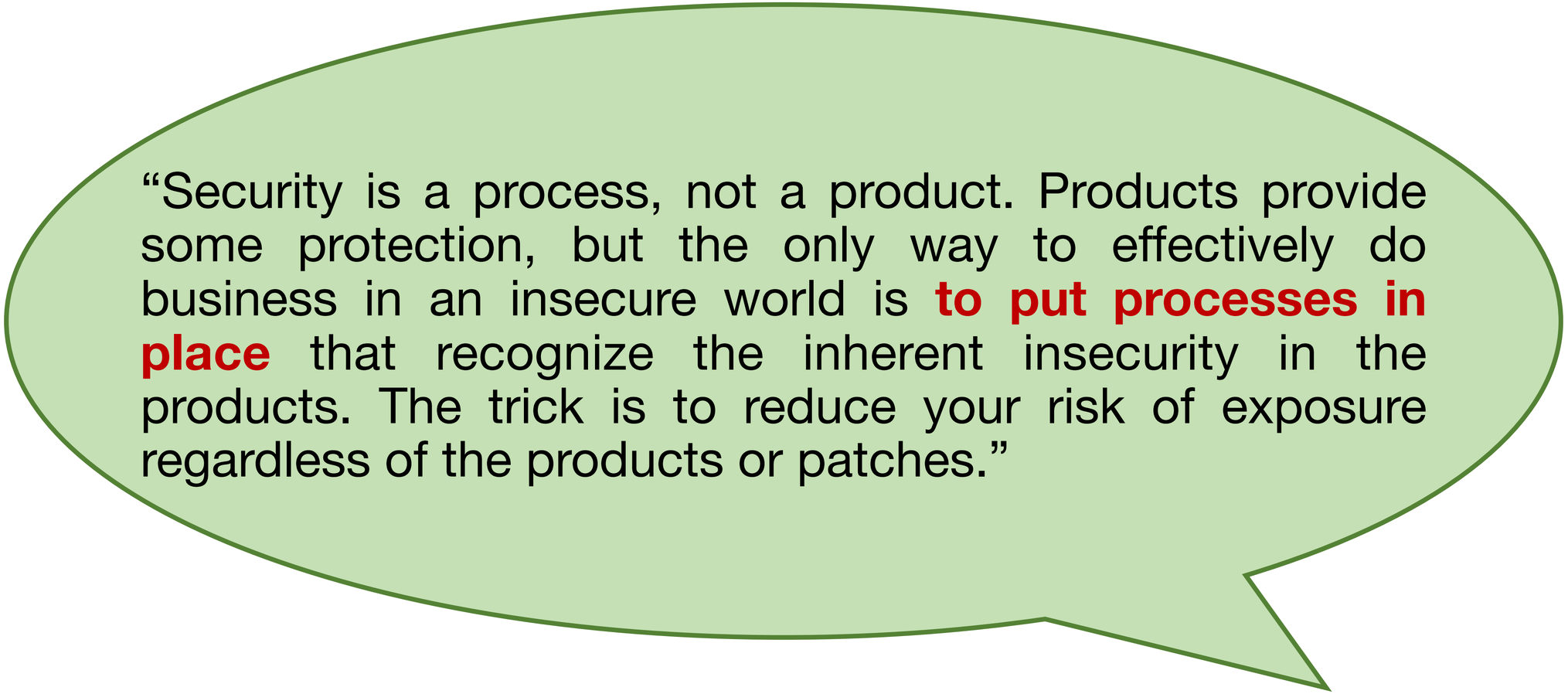
What do we know about security?

S4Lab

- Code security
- PKI/encryption
- Network security
- DB security
- System security

- All purely technical
- Fine-grained
- But what about the big picture?

However



"Security is a process, not a product. Products provide some protection, but the only way to effectively do business in an insecure world is **to put processes in place** that recognize the inherent insecurity in the products. The trick is to reduce your risk of exposure regardless of the products or patches."

[https://www.schneier.com/essays/archives/2000/04/the_process_of_secur.html]

What do we know about security?

S4Lab

- Code security
- PKI/encryption
- Network security
- DB security
- System security

- All purely technical
- Fine-grained
- But what about the big picture?

- What we don’t know about security?
  - The bigger picture
  - Do we cover the big big picture?
    - It is really not a flat domain
    - Too many factors to consider, and security is one of the elements

We (Engineers) are part of the problem!

S4Lab

Of the three components of cybersecurity—people, processes, and technology—technology is the viewed as the "easy button" because in relative terms, it's simpler than drafting a policy with the right balance of flexibility and specificity or managing countless organizational principles and human behavior.

Michael South, Amazon team

And we think buttons are the most complicated part!

The course structure

S4Lab

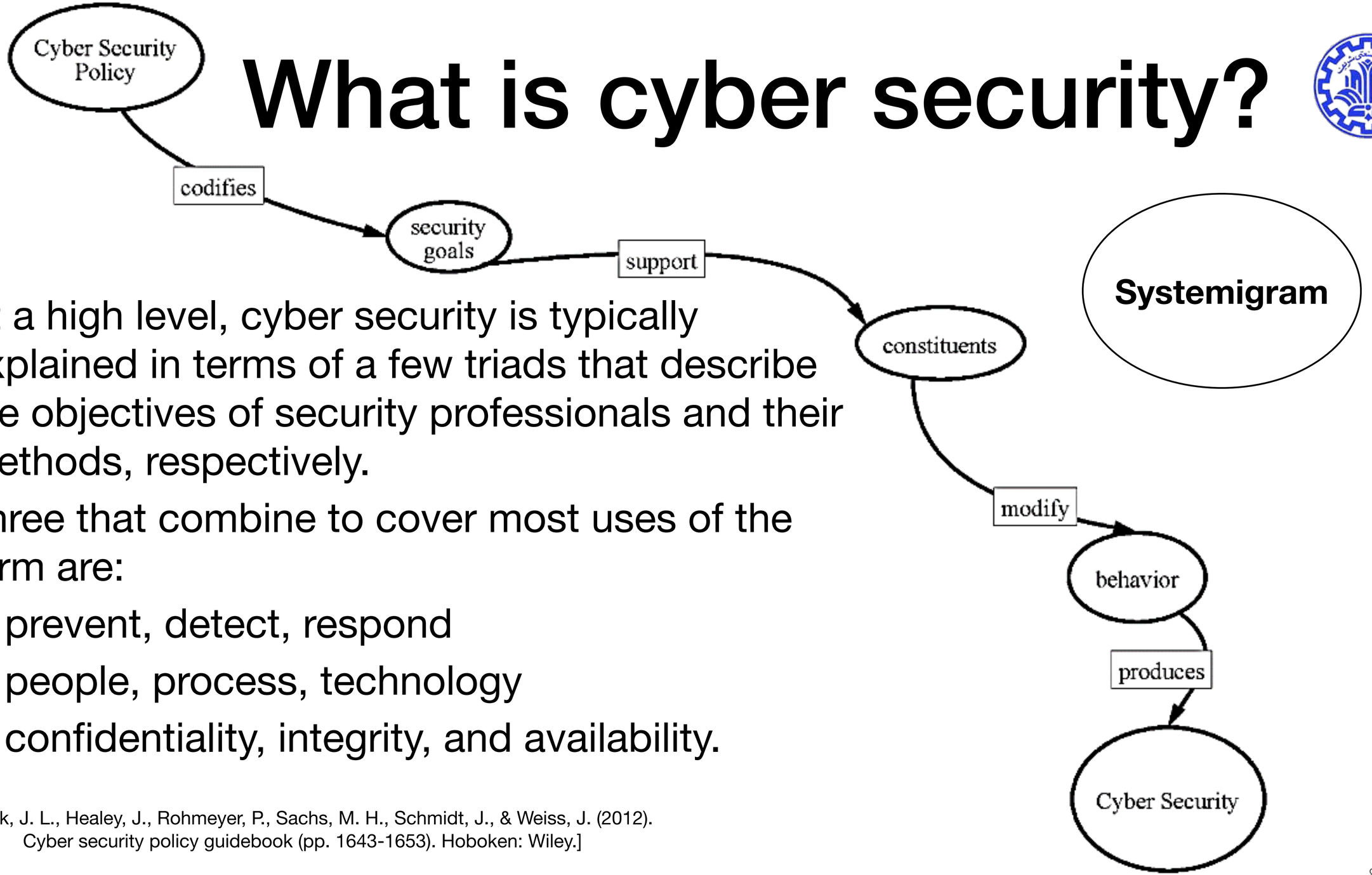
- Personal security policies
- Enterprise security policies
- National security policies
- International security policies

The course structure

S4Lab

- Personal security policies
- Enterprise security policies
- National security policies
- International security policies
- Is this nested view correct all the time?

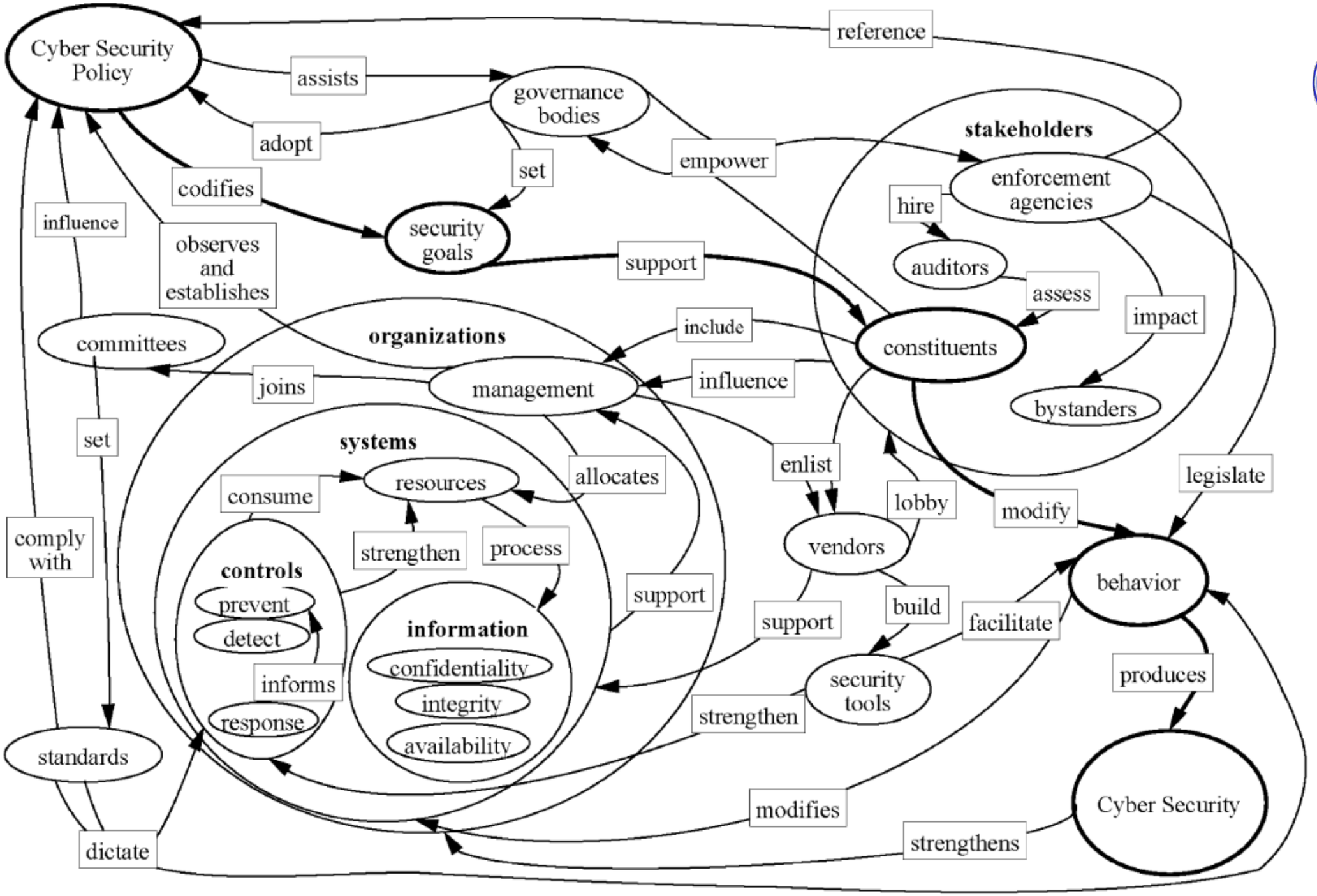
What is cyber security?



- At a high level, cyber security is typically explained in terms of a few triads that describe the objectives of security professionals and their methods, respectively.
- Three that combine to cover most uses of the term are:
  - prevent, detect, respond
  - people, process, technology
  - confidentiality, integrity, and availability.

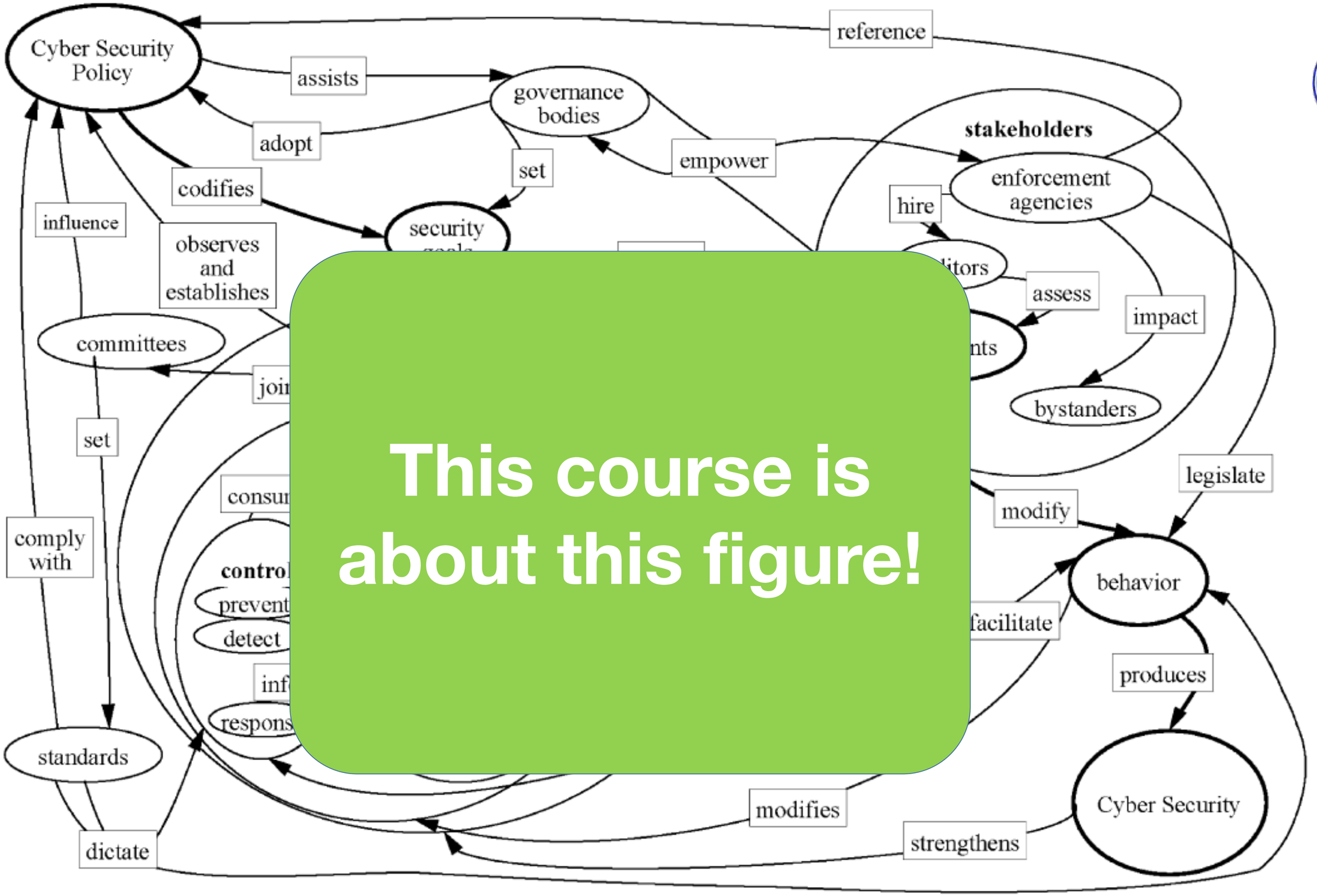
[Bayuk, J. L., Healey, J., Rohmeyer, P., Sachs, M. H., Schmidt, J., & Weiss, J. (2012). Cyber security policy guidebook (pp. 1643-1653). Hoboken: Wiley.]

Perspectives of cyber security



[Bayuk, J. L., Healey, J., Rohmeyer, P., Sachs, M. H., Schmidt, J., & Weiss, J. (2012). Cyber security policy guidebook (pp. 1643-1653). Hoboken: Wiley.]

Perspectives of cyber security



This course is about this figure!

[Bayuk, J. L., Healey, J., Rohmeyer, P., Sachs, M. H., Schmidt, J., & Weiss, J. (2012). Cyber security policy guidebook (pp. 1643-1653). Hoboken: Wiley.]

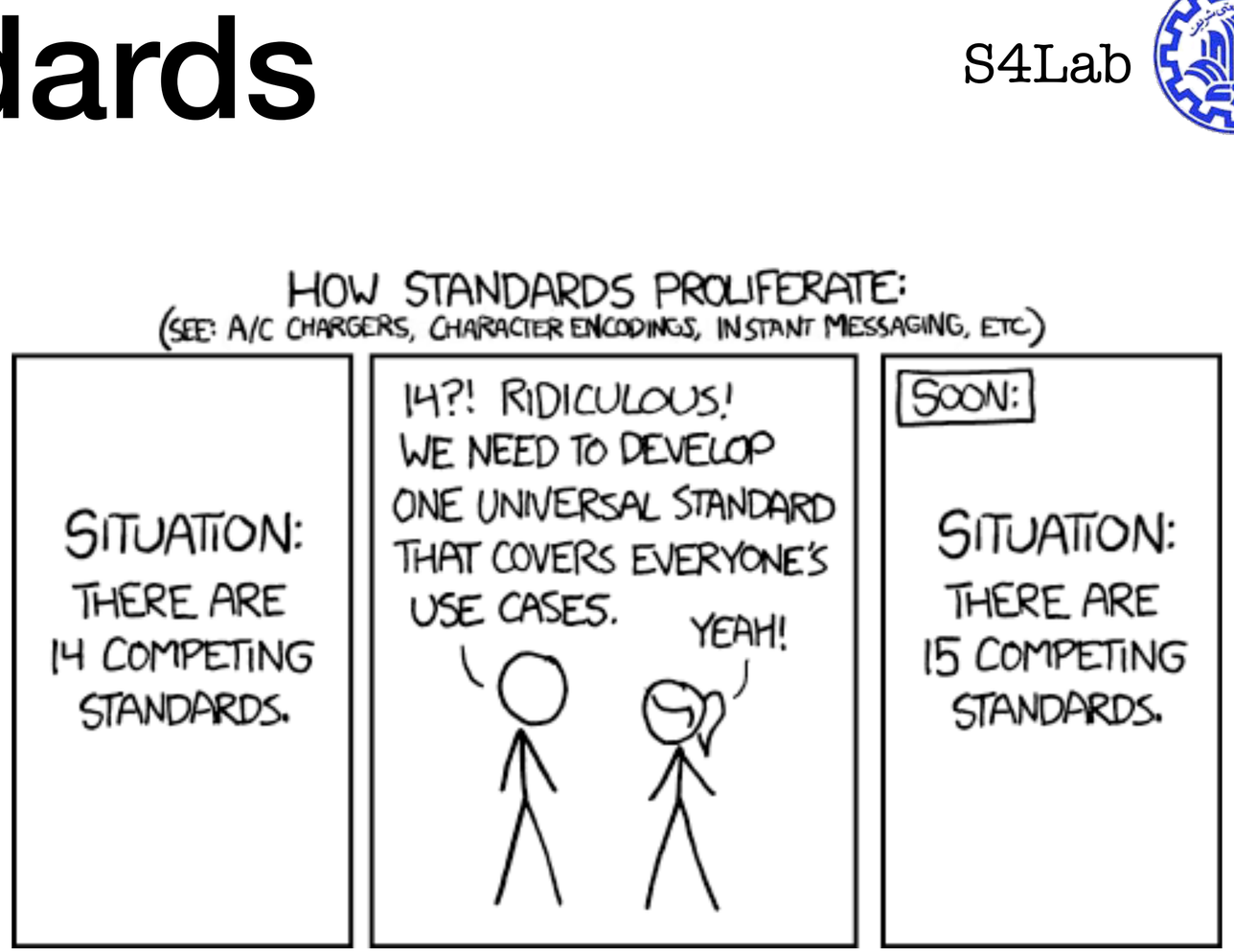
Why advantages?

S4Lab

- So we are going to talk about cyber policies at different levels
- Previous courses help you understand security mechanisms
- What if you want to work as a Security Architect?
  - For a company ? For an organization?
- Lack of a link between technical and governance issues in security community
- Let’s see some examples

Security standards

S4Lab



- Can you enumerate some?
- What are standard choices at each security subdomain?
- How an enterprise should achieve compliance?
- What about security frameworks/guidelines/ regulations?
- When do we need a new standard/framework?!

[xkcd.com]

Laws and Regulations

S4Lab

- What do you think about the relation between cyber policies and laws/ regulations?

[Bayuk, J. L., Healey, J., Rohmeyer, P., Sachs, M. H., Schmidt, J., & Weiss, J. (2012). Cyber security policy guidebook (pp. 1643-1653). Hoboken: Wiley.]

Laws and Regulations

S4Lab

- What do you think about the relation between cyber policies and laws/ regulations?
- It is possible to have cyber security executive directives, laws, and regulations without having articulated a cyber security policy at all !
  - China/US examples

[Bayuk, J. L., Healey, J., Rohmeyer, P., Sachs, M. H., Schmidt, J., & Weiss, J. (2012). Cyber security policy guidebook (pp. 1643-1653). Hoboken: Wiley.]

Laws and Regulations

S4Lab

- What do you think about the relation between cyber policies and laws/ regulations?
- It is possible to have cyber security executive directives, laws, and regulations without having articulated a cyber security policy at all !
  - China/US examples
- A more basic question,
  - what is **cyber law**?
- Are Laws technology dependent?

[Bayuk, J. L., Healey, J., Rohmeyer, P., Sachs, M. H., Schmidt, J., & Weiss, J. (2012). Cyber security policy guidebook (pp. 1643-1653). Hoboken: Wiley.]

A Declaration of the Independence of Cyberspace

S4Lab

“Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind…

We have no elected government, nor are we likely to have one, so I address you with no greater authority than that with which liberty itself always speaks.

In the United States, you have today created a law, the Telecommunications Reform Act, which repudiates your own Constitution and insults the dreams of Jefferson, Washington, Mill, Madison, DeToqueville, and Brandeis. These dreams must now be born anew in us.”

John Perry Barlow,
Davos, Switzerland
February 8, 1996

Law of the Horse

“We are at risk of multidisciplinary dilettantism, or, as one of my mentors called it, the cross sterilization of ideas. Put together two fields about which you know little and get the worst of both worlds.

The best way to learn the law applicable to specialized endeavors is to study general rules. Lots of cases deal with sales of horses; others deal with people kicked by horses; still more deal with the licensing and racing of horses, or with the care veterinarians give to horses, or with prizes at horse shows. Any effort to collect these strands into a course on 'The Law of the Horse' is doomed to be shallow and to miss unifying principles”

Frank H. Easterbrook

WHAT CYBERLAW MIGHT TEACH

“If you walked into a store, and the guard at the store recorded your name; if cameras tracked your every step, noting what items you looked at and what items you ignored; if an employee followed you around, calculating the time you spent in any given aisle;…You would notice and could then make a choice about whether you wanted to shop in such a store….

Hence law faces a choice— whether to regulate to change this architectural feature, or to leave cyberspace alone and disable this collective or individual goal."

Lawrence Lessig

Common approaches to cyber security

S4Lab

1. CYBER SECURITY AS DATA PROTECTION
   - Concerned with the protection of sensitive and personal data and communications, or otherwise confidential information to be protected from interception and wiretapping.
   - Is closely related to privacy concerns.
   - E.g. the case of Apple vs. the FBI in 2016

[Fichtner, L. (2018). What kind of cyber security? Theorising cyber security and mapping approaches. Internet Policy Review, 7(2), 1-19.]

Common approaches to cyber security

S4Lab

2. CYBER SECURITY AS SAFEGUARDING FINANCIAL INTERESTS
   - Protecting financial assets or securing commercial revenues.
   - E.g. Digital Millennium Copyright Act

[Fichtner, L. (2018). What kind of cyber security? Theorising cyber security and mapping approaches. Internet Policy Review, 7(2), 1-19.]

Common approaches to cyber security

S4Lab

3. CYBER SECURITY AS THE PROTECTION OF PUBLIC AND POLITICAL INFRASTRUCTURES
   - Where politicians and public policy officials talk about cyber security, they often speak about the protection of public, sometimes vital, infrastructures such as communication systems, electric grids, hospitals and public transport.

[Fichtner, L. (2018). What kind of cyber security? Theorising cyber security and mapping approaches. Internet Policy Review, 7(2), 1-19.]

Common approaches to cyber security

S4Lab

4. CYBER SECURITY AS CONTROL OF INFORMATION AND COMMUNICATION FLOWS
   - The final approach to cyber security presented can at times appear antagonistic to the other approaches.
   - It is often more concerned with breaking into systems than with protecting against breaches.
   - There are two separate aspects involved:
     - one is surveillance of communications and collection of intelligence in order to identify potential threats.
     - second is utilizing surveillance in order to directly moderate and censor information shared online.

[Fichtner, L. (2018). What kind of cyber security? Theorising cyber security and mapping approaches. Internet Policy Review, 7(2), 1-19.]

About the course

S4Lab

- Grading policy is as follows. This is tentative.
  - 30% Active participation in discussions
  - 40% Homeworks
  - 30% Final

Further reading

S4Lab

- Technologists vs policymakers
  - https://www.schneier.com/essays/archives/2020/02/technologists_vs_pol.html
- We will discuss this on discord (part of your class activity evaluation)

Reading for next session

S4Lab

- https://www.crowdsupply.com/sutajio-kosagi/precursor
- Bootstrapping Trust in Commodity Computers, Bryan Parno, Jonathan M. McCune, and Adrian Perrig Proceedings of the IEEE Symposium on Security and Privacy, May, 2010 (The paper, not the book!)