CSCI 1800 Cybersecurity and International Relations

Course Overview

John E. Savage

Brown University

Administrative Issues

- Introductions to the course TA staff
- Announcement of class meetings
  - Lectures – Mondays & Wednesdays in 85 Waterman Street, Room 130
  - Weekly sections – sign up soon
  - With instructor – after class & by appointment
- Collaboration policy
  - Please read Brown’s Academic Code

Course Introduction

- Cyberspace is the global network of computers. It includes clouds, control systems, & smart phones.
  - The Internet arrived on January 1, 1983.
  - Cyberspace emerged with the browser around 1991.
  - It is powered by algorithms – recipes for computations.
- We explore technological, policy, social, economic, international & security dimensions of cyberspace.
- Note: Social media algorithms want users to stay
  - Unanticipated use: political influence operations

Categories of Course Topics

- Technology/Policy Overview
  - Introduction to these topics
- Security
  - Crime, confidentiality, integrity, conflict
- Economics
  - Employing its levers; impact of CS on economics
- Governance
  - Roles for individuals, organizations, and governments
- Contemporary Topics
  - Disinformation, intelligence, software security, conflict

Assignments

	Points
• Three short response papers	45
• Final paper on a topic of your choice	35
• Nine sections	20
– Discussions of current topics	
– Team situation analyses (more later)	
	100

Overview of Today’s Lecture

- Introduction to the Internet
- Internet Naming and Routing
- The Hazards of Internet Globalization
- Internet Attacks
- Policy Responses
- Outline of the course

Introduction to the Internet

The Ubiquitous Internet

- Internet is revolutionizing commerce, changing cultures, engaging governments, and ubiquitous

The Global Cyber Challenge

- Cyberspace is an important but challenging place
  - Almost all of us are very dependent upon it
  - Critical resources are now accessible
  - Theft, disinformation, and espionage are rampant
- Our challenge is to make it more secure.
  - If we fail crime and disruptions will increase, and
  - Conflict may result
- To address these challenges
  - We need people who understand policy and technology

Note

- This course is designed for non-specialists
- Computer science students will learn policy
- Policy students will learn a bit of technology
- The goals:
  - Develop a basic understanding of the issues
  - Acquire skill in crossing technology/policy divide

Encoding Data with Bits and Packets

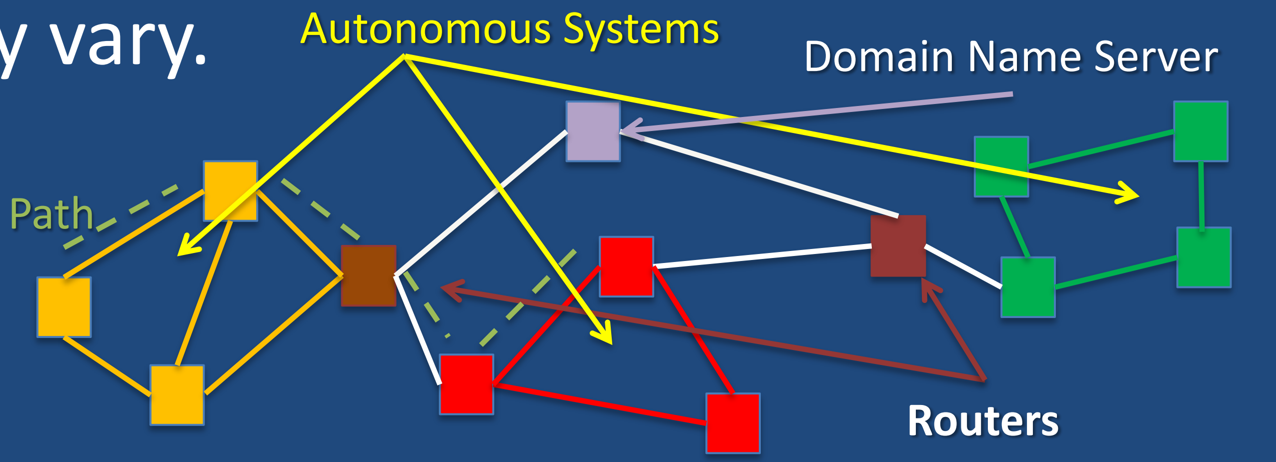
- An image consists of rows of pixels, say 640 by 480
- Each pixel typically consists 3 colored dots, RGB
- Intensity of dots (bits per dot) determines color (0,1)
- An image is specified by a long sequence of bits
- To transmit, bits grouped into packets, e.g. 1024 bits.

Counting Patterns of Bits

- 0, 1 (2)
- 00, 01, 10, 11 (4)
- 000, 001, 010, 011, 100, 101, 110, 111 (8)
- 0000, 0001, 0010, 0011, 0100, 0101, 0110, 0111, 1000, 1001, 1010, 1011, 1100, 1101, 1110, 1111 (16)
- 32 5-bit patterns; 64 6-bit patterns;
- 128 7-bit patterns

What is the Internet?

- Collection of networks, each run by an autonomous system – a manager of IP addresses.
- Data streams broken into IP packets and routed using an Internet protocol. Paths taken by IP packets may vary.



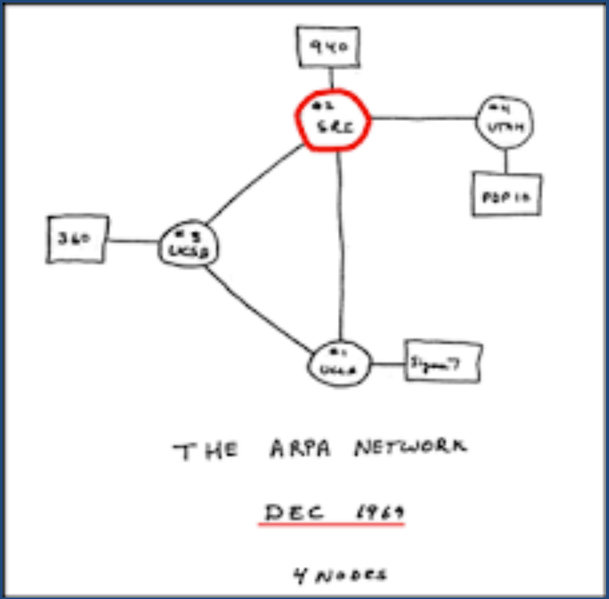
Three networks, two routers, and one domain name server (DNS)

The Internet Has Become Wild West

- The gunslingers – Hackers
- The town – Hundreds of millions of marginally protected computers
- Where are the sheriffs?
  - We once slapped a badge on a hacker & expected to be protected.
- How do we protect ourselves and our assets?
- How do we know if we are protected?

History of the Internet

- First public switched telephone network (PSTN) built in 1875 – communicates via fixed paths
- Packet networks invented in US & UK in 1960s.
- Experiments begin in US in 1970s and 80s.



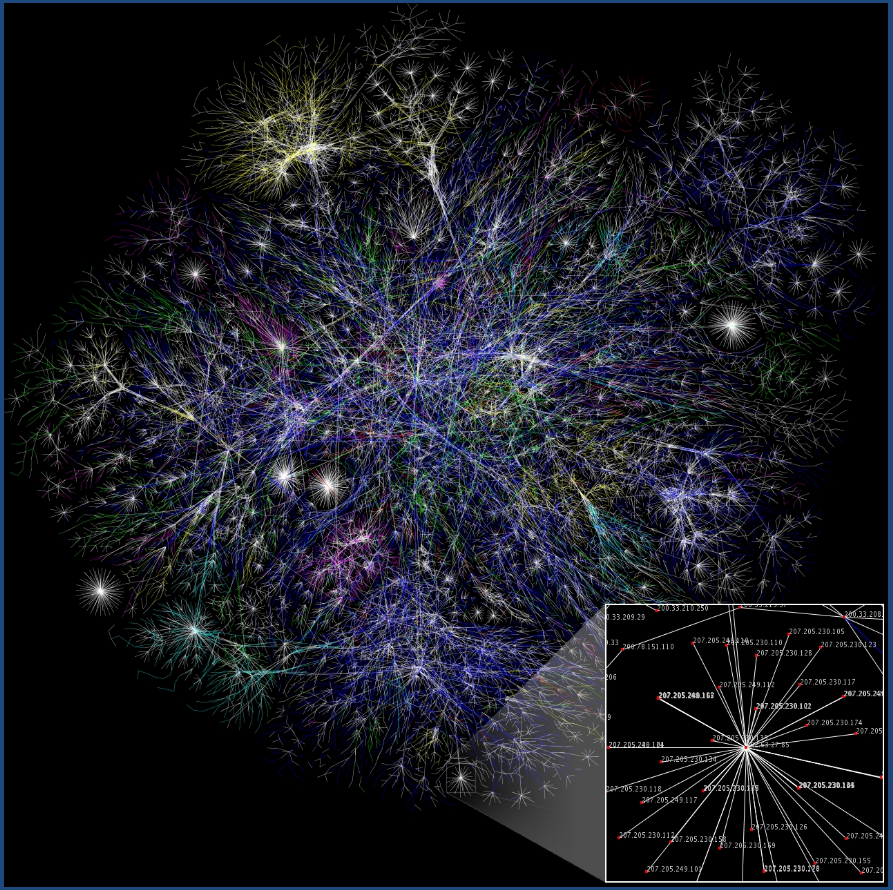
ARPANET as envisioned in ‘69

History of the Internet

- Basic packet transmission protocol, TCP/IP, adopted by US military on January 1, 1983.
  - Other packet switched protocols lose out to Internet
  - Network effect – when a technology achieves market dominance, others die off
- Internet fully emerges in 90s with introduction of browsers and the World Wide Web.
- Explosive growth follows.

The Internet Today

- ~60K autonomous systems (subnetworks)
- ~30 billion connected devices in 2019
- The Internet is an integral element in the world economy.



Lect01 1/22/2020

Why is the Internet So Effective?

- All the intelligent technology is at the periphery.
  - In the phone network the smarts are inside
  - Networks are controlled by monopolies
- Initially no one controlled the Internet
  - It is now heavily regulated in autocratic countries
  - US and others like its openness but now worried
- The Internet standards process is wide open!
  - Governed by a multi-stakeholder process.

Internet Naming and Routing

The Domain Name System (DNS)

- Each packet has source & destination IP address
  - Addresses are needed to get to destinations and back
  - An address is a string of 32 (IPv4) or 128 (IPv6) bits.
- Because IP addresses hard to remember, humans use domain names, such as www.brown.edu.
- The DNS is the phone book for the Internet

How Does the Internet Work

- www.brown.edu translates into 128.148.128.180 which is an IPv4 32-bit address.
- Each number represent 8 bits (4x8 = 32)
- If your computer doesn’t know the IP address, it contacts a DNS Resolver that asks questions:
  - Root zone server, who manages .edu?
  - .edu manager, who manages brown.edu? Etc.
  - www.brown.edu manager, what’s your IP address?

Hazards of Internet Globalization

Globalization Introduces Risks

- Efficiency encourages migration of applications to the Internet.
  - Critical infrastructures are now connected
- Global Internet makes local resources accessible remotely.
  - Miscreant in country A can cause mischief in B.
- Cost of efficiency is increased risk!

Critical Infrastructure

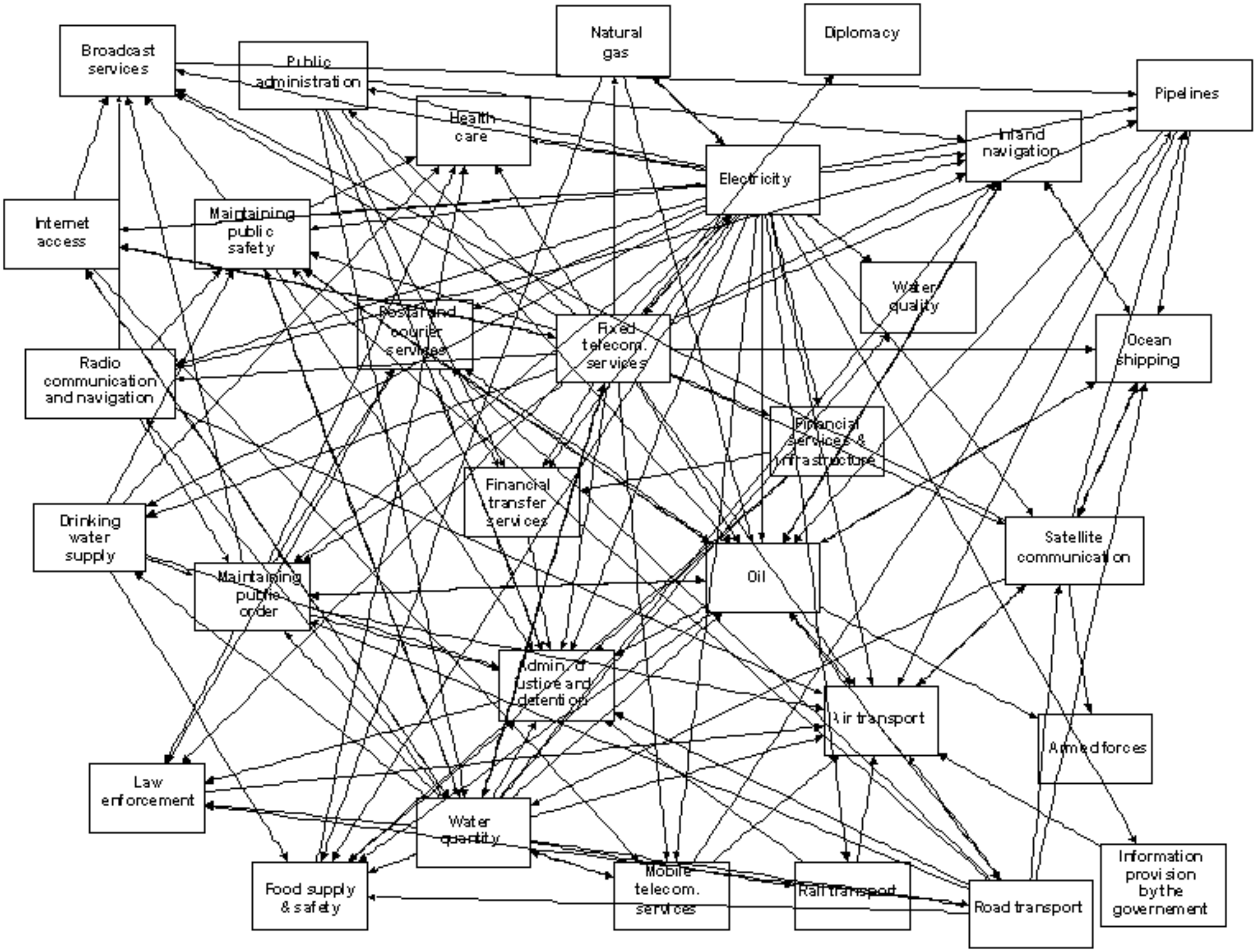
- Financial and banking systems
  - Federal Reserve Bank of Boston handles > $5 trillion of transactions per day!
  - > $10 trillion/day of wire transfers via undersea cables
    - Data is not in the clouds, it is in the ocean (https://www.nytimes.com/interactive/2019/03/10/technology/internet-cables-oceans.html)
  - Compare this to US GDP which is $21 trillion/year
- Power grid is highly vulnerable to attack.
  - Russia attacked Ukraine grid in 2015 and 2016.
  - Approximately 3,300 US companies provide electricity

16 US Critical Infrastructure (CI) Sectors

Chemical	Commercial Facilities	Communications
Critical Manufacturing	Dams	Defense Industrial Base
Emergency Services	Energy	Financial Services
Food and Agriculture	Government Facilities (includes electoral systems)	Healthcare and Public Health
Information Technology	Nuclear Reactors, Materials, and Waste	Transportation Systems
Water and Wastewater		

See https://www.dhs.gov/critical-infrastructure-sectors

Interdependencies of the CI



Lect01 1/22/2020

Source: Dutch TNO

SCADA Systems Are in CI

- SCADA: Supervisory control & data acquisition
- These systems control power, water, etc.
- They were not designed to be secure
  - Some have hard coded passwords
  - Many are connected to Internet
- Many SCADA systems are fragile.
  - They use feedback to maintain steady state
  - Large changes can cause cascading failures.

Opinions on Internet

- Pres. **Obama**[1]:
  - – "… our interconnected world presents us, at once, with great promise but also great peril."
- Former Dir. National Intelligence **McConnell**[2]:
  - – "As the most wired nation on Earth, we offer the most targets of significance, yet our cyber-defenses are woefully lacking. … The problem is that we lack a cohesive strategy to meet this challenge."

1. Remarks on May 29, 2009
2. Washington Post, February 28, 2010

Examples of Damage

- Mandiant Corp 2013 profile of government hackers:
  - PLA 3rd Department Unit 61398 in Shanghai responsible for stealing terabytes of data from ≥ 141 orgs since 2006.
  - Maintained access to computers for average of 356 days!
- Good news: In 2016 Crowdstrike reported a 94% drop in theft of intellectual property for commercial use after US/China agreement of 9/15.
- Bad news: In 2018 theft back to 2015 levels!
- Kaspersky Lab estimates Carbanak crime ring stole > $1B since 2013 from > 100 banks in 30 nations!
- Snowden reveals NSA global surveillance in 2013!
- Ransomware now a billion dollar business!

Internet Attacks

Three Types of Internet Attack

- Seize control of a computer
  - Exploit a software hole or phish a user & load backdoor
  - Attacks can occur via email, browser, USB, CDs, IM, Twitter
  - Top 10 vulnerabilities account for 85% of break-ins, some old.
- Distributed denial of service (DDoS) attack
  - Send many packets to one computer, overwhelming it
- Routing attacks
  - Redirect users to malicious web sites
  - 12/10/18 Google lost control of millions IP addresses to China

Outline of a Typical Attack

- A target clicks on link from “trusted” source.
  - Link contains code which is run, giving attacker access to his/her user computer, or
  - Link connects to website that has malicious payload,
- Browser downloads and runs malicious payload that gives attacker access to machine.
- Attacker now has complete control of computer
- Attacker can steal or change intellectual property or damage attached equipment.

Stuxnet – First Cyber Weapon

- Sophisticated and complex worm that emerged in July, 2010. Infected more than 100,000 hosts.
- Targeted Iranian nuclear fuel refinement facility.
  - Destroyed almost 1,000 centrifuges!
  - President Ahmadinejad acknowledged the attack.

- Flame – data collection for Stuxnet, etc.
  - Highly complex and huge – 20 Megabytes of code!

Networks Are Also Vulnerable

- Border Gateway Protocol† (BGP)
  - Used by autonomous systems (AS) to invite traffic.
  - It plays a vital role in routing Internet traffic.
  - Based on trust. It has been misused to disrupt traffic
- Some Global Internet Traffic Disruptions
  - Feb 24, 2008 – For about two hours connection lost to YouTube due to action by Pakistan Telecom
  - April 8, 2010 –For 18 mins routes to 32,000+ networks sent to China Telecom, affecting Facebook, Twitter, etc

† See WaPo article on BGP: http://www.washingtonpost.com/sf/business/2015/05/31/net-of-insecurity-part-2/

How Did This Mess Develop?

- Market forces have led to monocultures
  - Common operating systems and applications in use.
  - Result: Network is as weak as its weakest link.
- We concentrate resources for efficiency
  - Internet has too many choke points.
  - Cloud computing is popular – saves time and energy – but centralizes data/programs, providing big target. However, can be more secure than home computers
  - 99% of international Internet traffic on undersea cables

Policy Responses

Characteristics of the Internet[1]

- Provides global reach, but based on trust
  - Need confidence that domains can be reached and that confidentiality not violated
- Permission-less innovation
  - Ability to create new services without permission
- Accessibility
  - Easy to add content or attach new server to network
- Spirit of collaboration
  - Multiple stakeholders cooperate

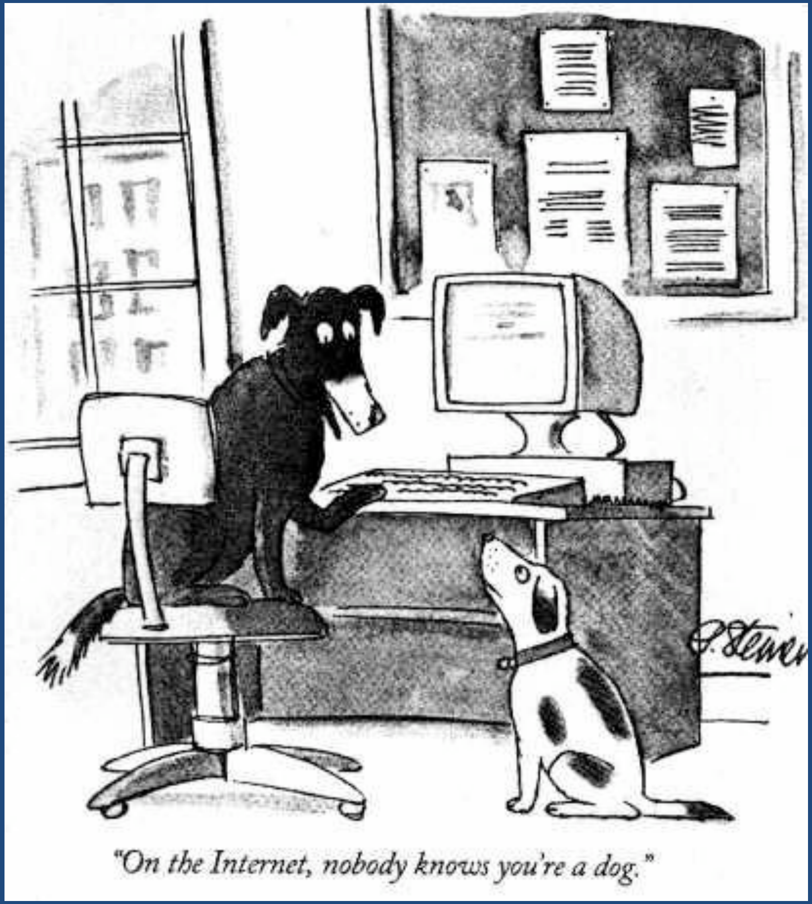
[1] Based on speech by Sally Wentworth At Dutch Embassy, Wash DC 2/21/12

Policy Goals for Cyberspace

- Preserve best features of Internet
  - Requires education, trust development, negotiations
  - Establish norms of state behavior
  - Protect privacy, civil liberties and national interests
- Improve cyber defenses
  - Make computers and networks more secure
  - Employ best practices individually and collectively
  - Engage in risk reduction locally and internationally

Attribution

- To respond to miscreants
  - We need attribution with very high assurance, but difficult to obtain
  - Retaliation may cause collateral damage and an unpredictable response.



On the Internet, nobody knows your’e a dog.

What Should Nations Do?

- Develop domestic legislation to
  - Encourage/require improved vendor cybersecurity
  - Share threat information between organizations/govts
  - Develop cyber insurance – have experts assess sites
- Formulate Internet governance strategies
  - Work with most influential governments
  - Work with Internet users
- Fund research and development on
  - Cybersecurity technology
  - Policy formulation

There is Hope for Better Security

- Leap-ahead technologies are promising
  - Apply techniques to thwart attackers
  - Develop economic incentives to improve security
  - Integrate secure identity management into systems
- Crypto computing may be possible
  - Encrypt data and programs so that computations can be done without decryption.
- Governments now engaged
  - Many meetings held and international centers set up

Course Outline

Lecture Topics

- Intro to Technology & Policy Challenges
- Computer Hardware & Software
- Hardware and Software Vulnerabilities
- Design & Operation of the Internet
- Internet Naming and Routing Protocols
- Cyber Exploits
- Attribution and Privacy

Lecture Topics (cont.)

- Major Cyber Attacks
- Secure Communications and Authorization
- Cyber Conflict
- Bitcoin and Blockchains
- Cyber Economics
- Transborder Issues
- Internet Governance

Lecture Topics III

- The International Norms Process (Guest)
- Social Media and Propaganda (Guest?)
- AI and Ethics
- Engineering for Security
- Defense in Depth
- Future Directions

Situation Analysis

- A new exercise for this course.
- A small team (2-3) is given an ambiguous but serious threat.
- Students have to analyze it, assess its risks, and propose mitigations.
- This type of analysis is done by governments and the private sector.
- Cyber makes the problem more challenging.

Conclusion

- Cyberspace is a complex new medium.
- Slowly coming to grips with its challenges.
- Decades of research, policy development, legislation, and international negotiation will be required to tame cyberspace.
- It is a multidimensional problem requiring people who can cross boundaries.
- Course provides an intro to this exciting topic.