

CS558 Network Security

Lecture 1: Intro

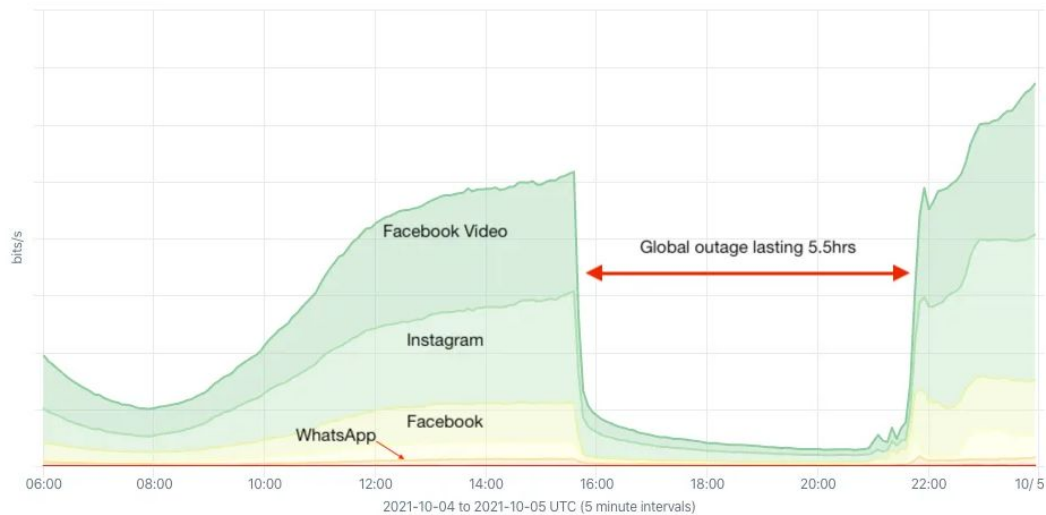
Course's Major Technical Themes

Course's Major Technical Themes

Computer Networks

Computer Security

Top OTT Service by Average bits/s Internet Traffic served by Facebook
Oct 04, 2021 06:00 to Oct 05, 2021 00:00 (18h) | Global outage 4-Oct-2021



Let's  Encrypt

Story 1: Corporate/National Defense



U.S. Army
Cyber Command



Fleet Cyber Command
(10th Fleet)



Sixteenth Air Force
(Air Forces Cyber)



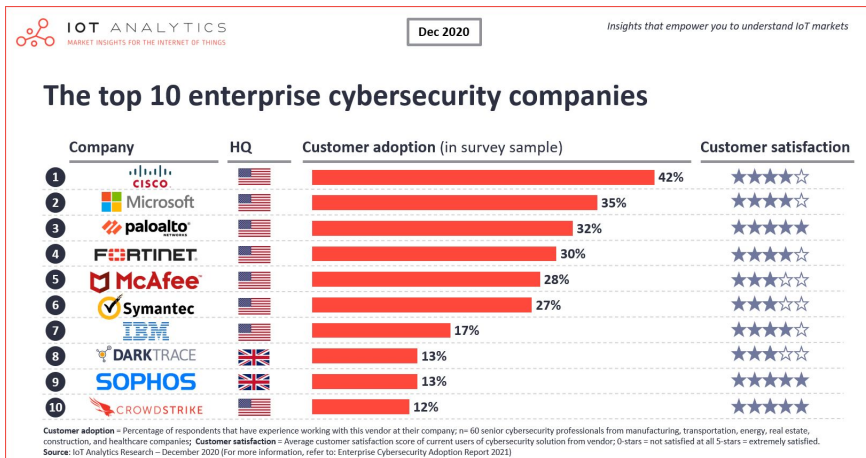
Marine Corps Forces
Cyberspace Command



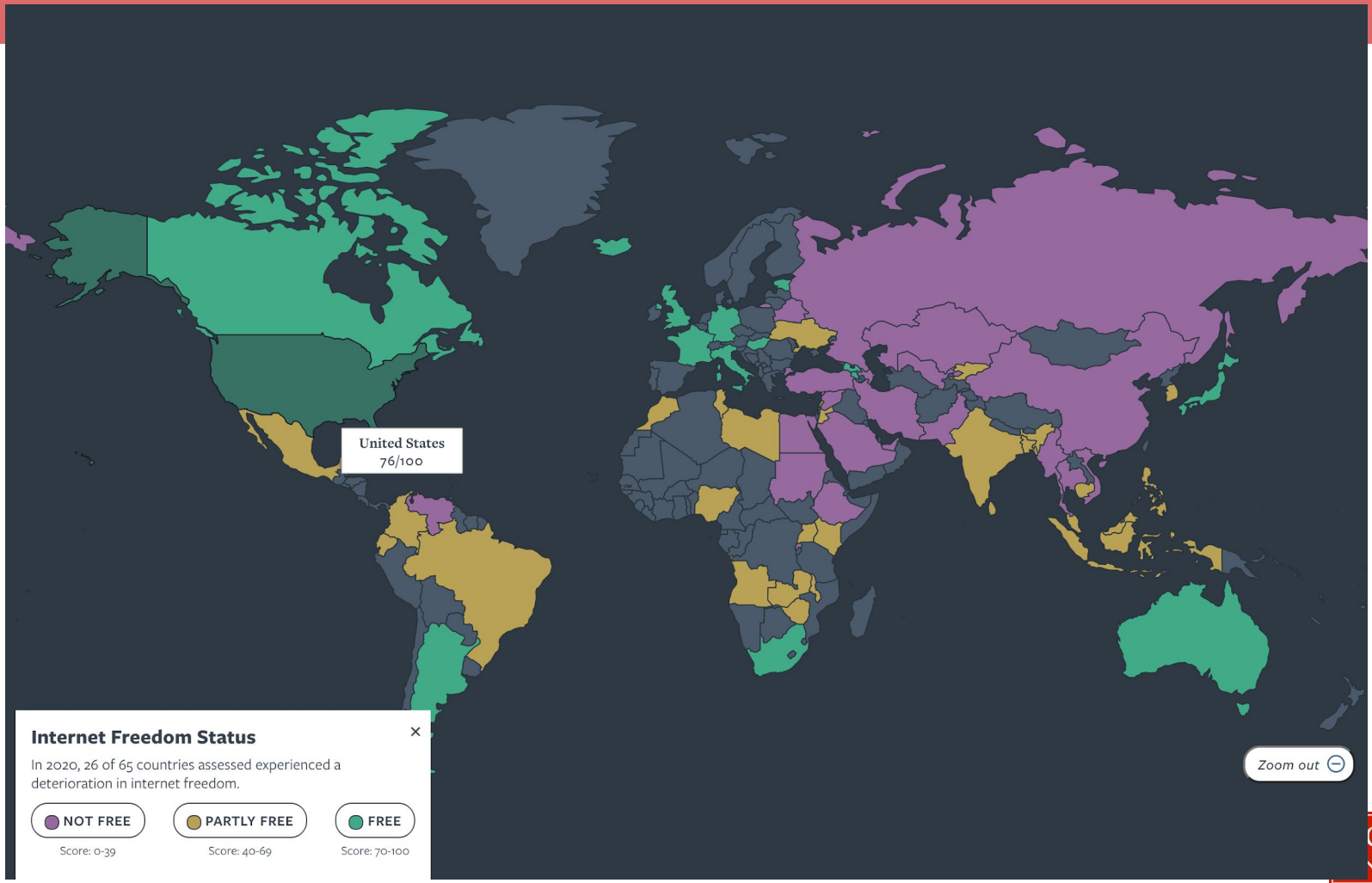
Cyber National Mission Force



Joint Force Headquarters -
DoD Information Network



Story 2: Civil Liberties and Surveillance



United States
76/100

Internet Freedom Status

In 2020, 26 of 65 countries assessed experienced a deterioration in internet freedom.

- NOT FREE**
Score: 0-39
- PARTLY FREE**
Score: 40-69
- FREE**
Score: 70-100

Zoom out

OPINION

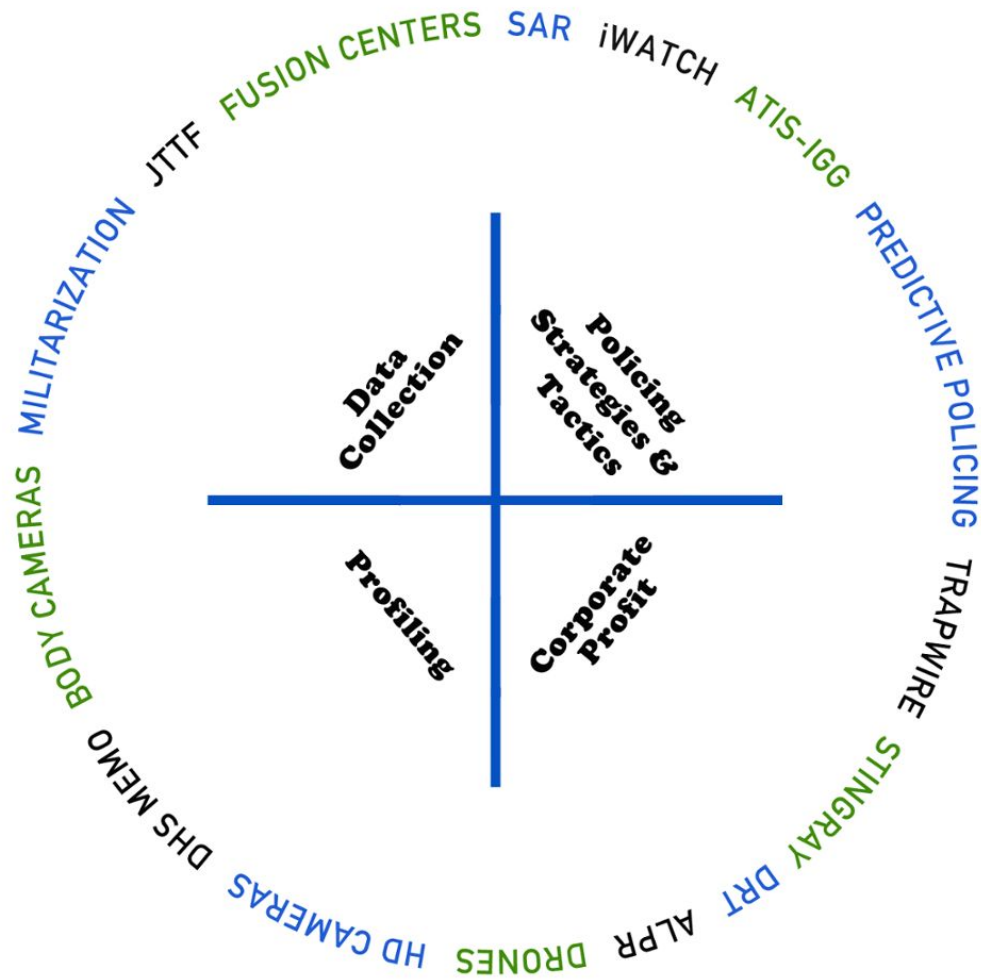
What It's Like to Live in a Surveillance State

By James A. Millward



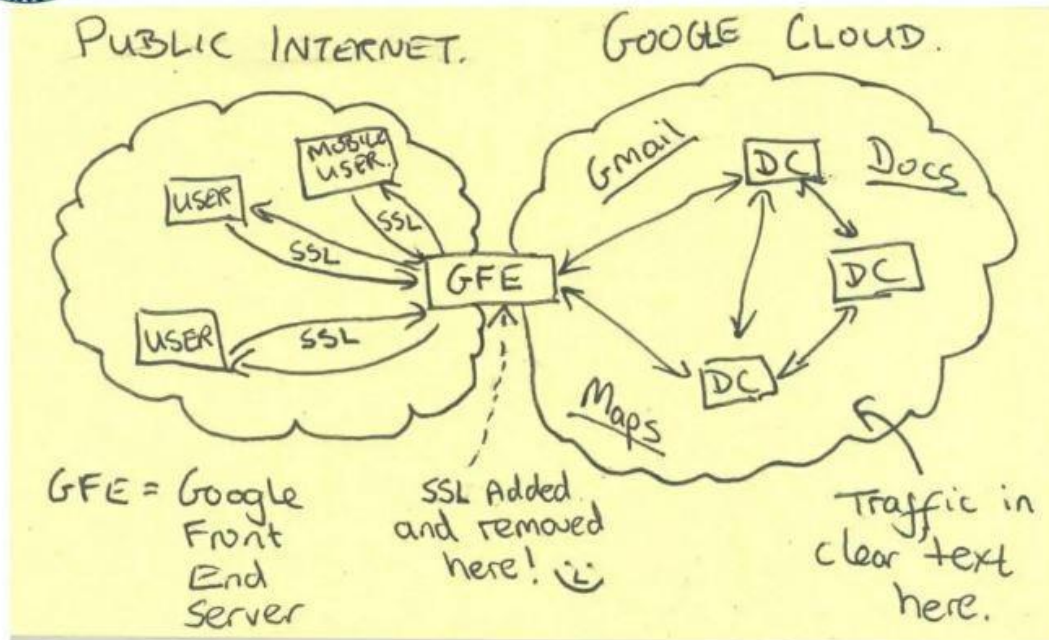








Current Efforts - Google



Public Law 107–56
107th Congress

An Act

Oct. 26, 2001
[H.R. 3162]

To deter and punish terrorist acts in the United States and around the world,
to enhance law enforcement investigatory tools, and for other purposes.

*Be it enacted by the Senate and House of Representatives of
the United States of America in Congress assembled,*

SECTION 1. SHORT TITLE AND TABLE OF CONTENTS.

(a) **SHORT TITLE.**—This Act may be cited as the “Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001”.

(b) **TABLE OF CONTENTS.**—The table of contents for this Act is as follows:

- Sec. 1. Short title and table of contents.
- Sec. 2. Construction; severability.

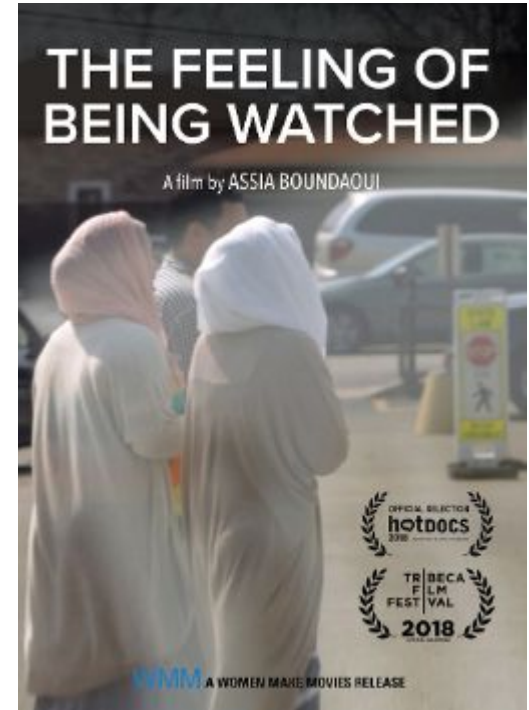
TITLE I—ENHANCING DOMESTIC SECURITY AGAINST TERRORISM

- Sec. 101. Counterterrorism fund.
- Sec. 102. Sense of Congress condemning discrimination against Arab and Muslim Americans.
- Sec. 103. Increased funding for the technical support center at the Federal Bureau of Investigation.
- Sec. 104. Requests for military assistance to enforce prohibition in certain emergencies.
- Sec. 105. Expansion of National Electronic Crime Task Force Initiative.
- Sec. 106. Presidential authority.

TITLE II—ENHANCED SURVEILLANCE PROCEDURES

- Sec. 201. Authority to intercept wire, oral, and electronic communications relating

Uniting and
Strengthening
America by
Providing
Appropriate
Tools Required to
Intercept and
Obstruct
Terrorism (USA
PATRIOT ACT)
Act of 2001.
18 USC 1 note.

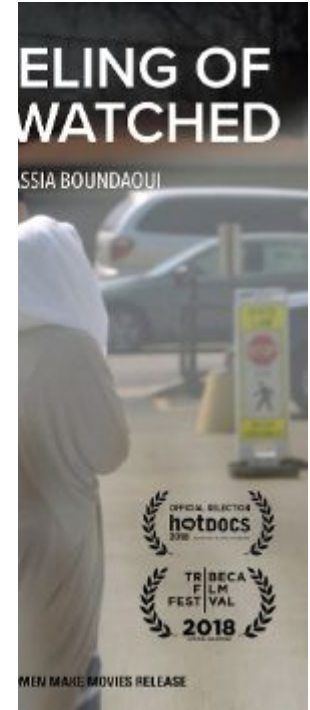


TITLE II—ENHANCED SURVEILLANCE PROCEDURES

- Sec. 201. Authority to intercept wire, oral, and electronic communications relating to terrorism.
- Sec. 202. Authority to intercept wire, oral, and electronic communications relating to computer fraud and abuse offenses.
- Sec. 203. Authority to share criminal investigative information.
- Sec. 204. Clarification of intelligence exceptions from limitations on interception and disclosure of wire, oral, and electronic communications.
- Sec. 205. Employment of translators by the Federal Bureau of Investigation.
- Sec. 206. Roving surveillance authority under the Foreign Intelligence Surveillance Act of 1978.
- Sec. 207. Duration of FISA surveillance of non-United States persons who are agents of a foreign power.
- Sec. 208. Designation of judges.
- Sec. 209. Seizure of voice-mail messages pursuant to warrants.
- Sec. 210. Scope of subpoenas for records of electronic communications.
- Sec. 211. Clarification of scope.
- Sec. 212. Emergency disclosure of electronic communications to protect life and limb.
- Sec. 213. Authority for delaying notice of the execution of a warrant.
- Sec. 214. Pen register and trap and trace authority under FISA.
- Sec. 215. Access to records and other items under the Foreign Intelligence Surveillance Act.
- Sec. 216. Modification of authorities relating to use of pen registers and trap and trace devices.

Oct. 26, 2001
[H.R. 3162]

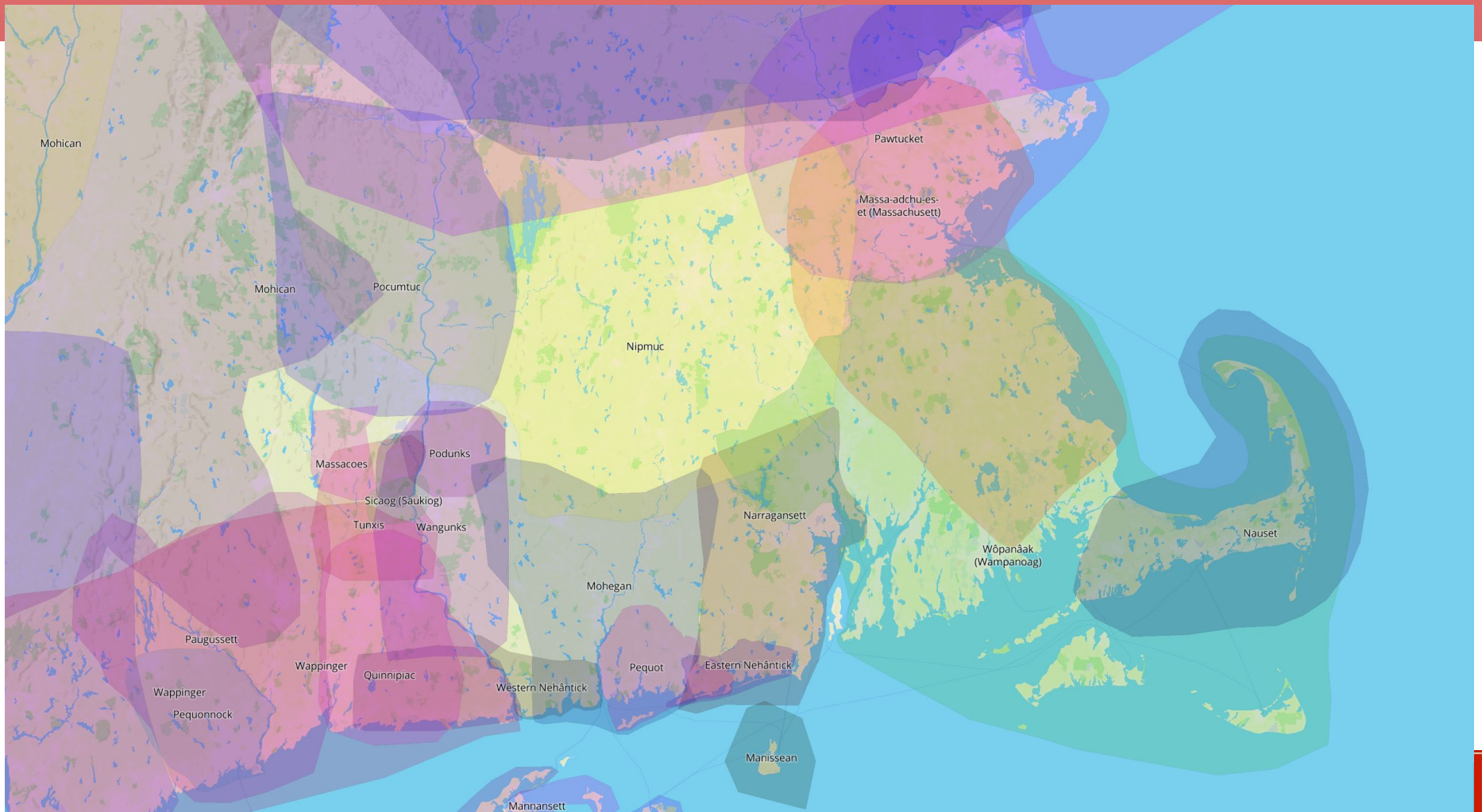
Uniting and
Strengthening
America by
Providing
Appropriate
Tools Required to
Interrupt and
Obstruct
Terrorism (USA
PATRIOT ACT)
Act of 2001.
18 USC 1 note.





“Cryptography rearranges power: it configures who can do what, from what. This makes cryptography an inherently political tool, and it confers on the field an intrinsically moral dimension.”

-- Phil Rogaway, “The Moral Character of Cryptographic Work,” 2015



Course Learning Goals

- Know and understand the fundamental tools that secure the modern internet
- Educated guess as to **WHY** components of secure protocol are there
- Develop/deepen adversarial thinking
- Strengthening independent learning skills

Course Outline

Part 1: When Networking Protocols Go Wrong

(Or, “Wait... what if someone doesn’t play nice?!?”)

- ARP, DNS, BGP, TLS.

Part 2: Privacy on the web

- Censorship Resistance (Tor, Accessing Tor)
- A little bit of secure messaging

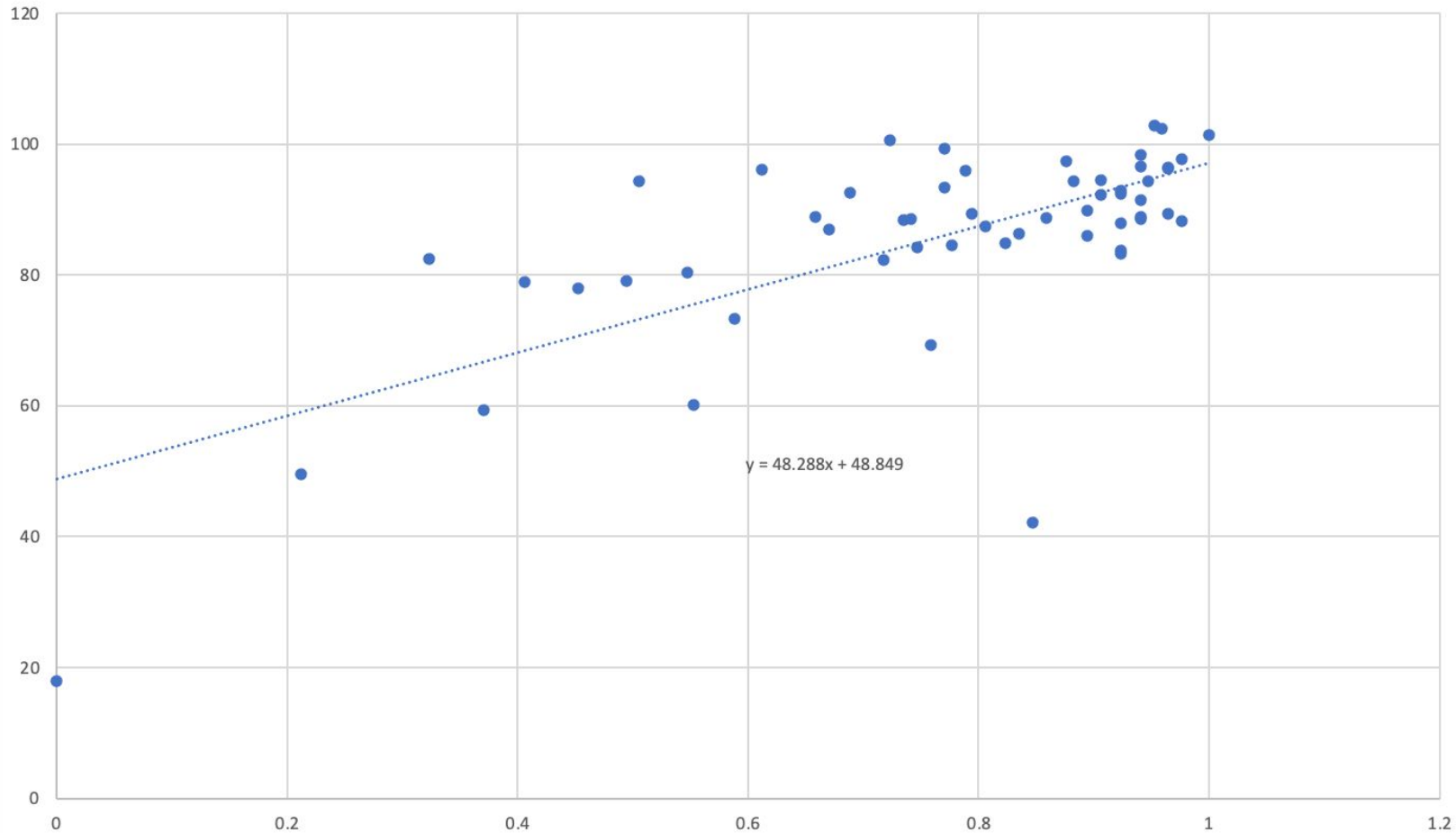
Course Logistics

- Piazza and Gradescope (<https://www.gradescope.com/courses/489834> Code: K3XEWR)
- Assignments (Mostly monday nights @9pm)
 - 3 Written Homeworks (30%)
 - 2 Programming Assignments (32%)
 - Cumulative Final Exam (25%)
 - Weekly Reading Assignments (15%)
 - Summary ~150 words
 - 1 thing you found interesting
 - 1 thing you found confusing
 - 1 thing you googled to learn more about
 - Weekly Question (3%) (Friday@9pm)
- Labs/Review Sections

What will be helpful to know?

- Crypto Basics
 - Symmetric Key Encryption
 - Public Key Encryption
 - Message Authentication Codes
 - Digital Signatures
 - Cryptographic Hash Functions
 - Pseudorandom Functions (will come up later and are less important)
- Crypto Homework
- Good High-level Understanding of Networking
- Python

Crypto Homework Grade vs Final Grade 2022



Things to know about me

- Applied Cryptography is my home
- Slides will make way more sense in context
- Can't spell to save my life
- Offline Friday night - Saturday night
- Office Hours