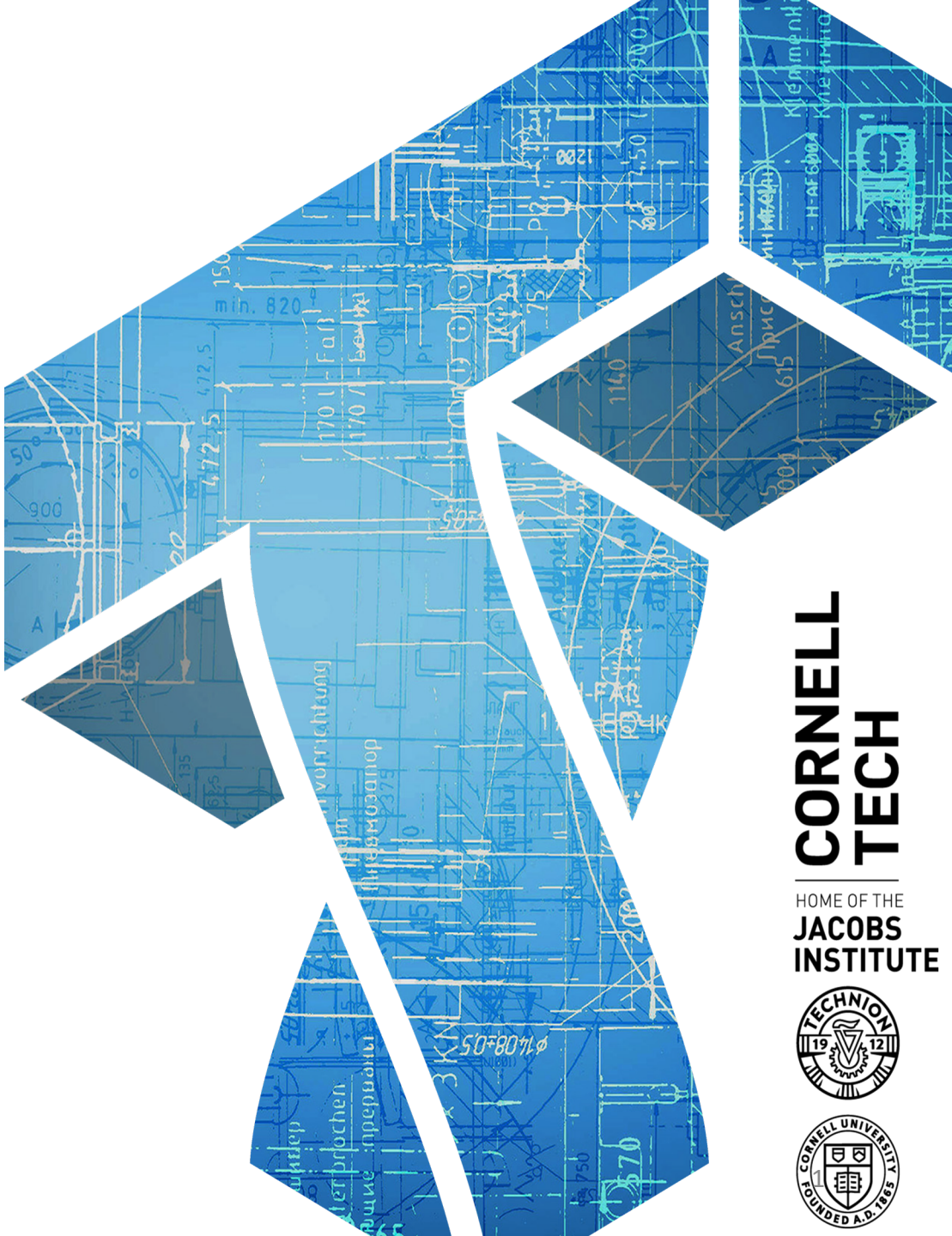
CS 5435: Computer security and government

Instructor: Tom Ristenpart

https://github.com/tomrist/cs5435-fall2019



CORNELL TECH
HOME OF THE JACOBS INSTITUTE

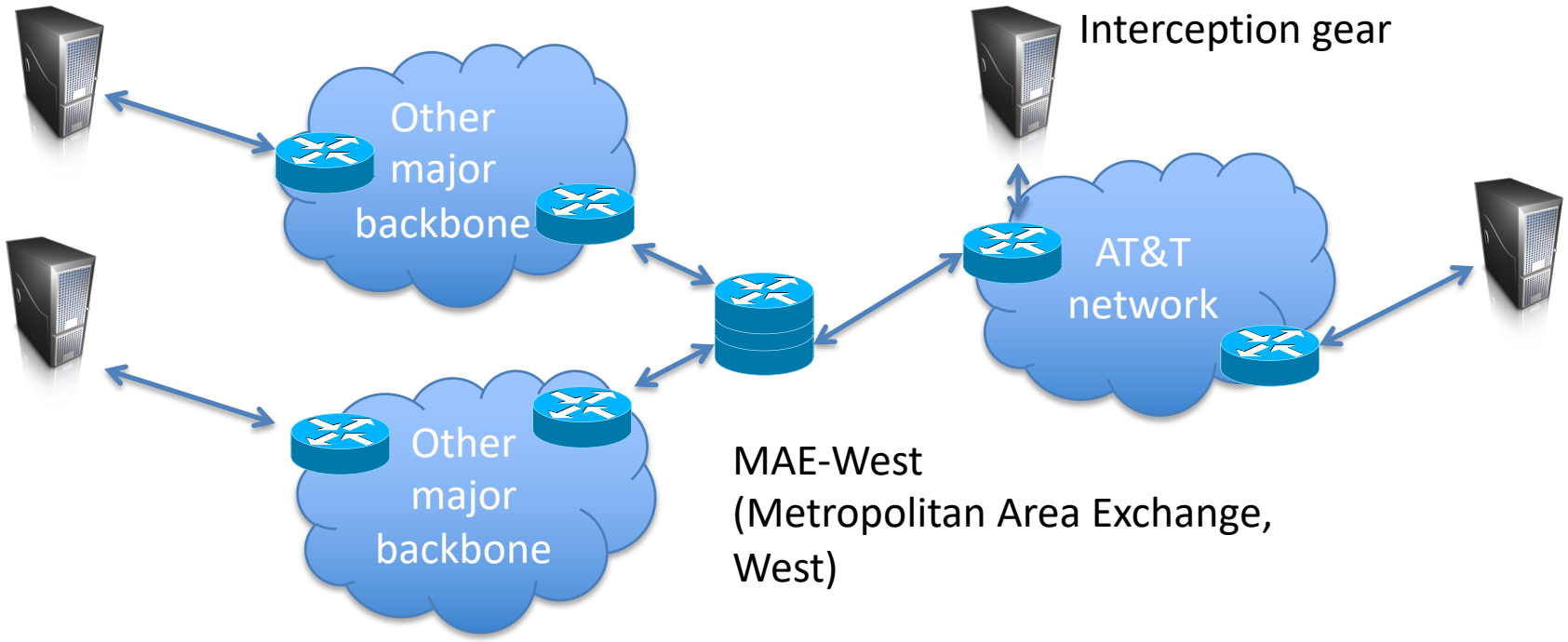
Topics for today

- Mass surveillance
- The “going dark debate”
- Internet censorship
- Targeted espionage

AT&T Wiretap case

- Mark Klein discloses potential wiretapping activities by NSA at San Francisco AT&T office in 2006
- Fiber optic splitter on major trunk line for Internet communications
  - Electronic voice and data communications copied to “secret room”
  - Narus STA 6400 device

Wiretap surveillance

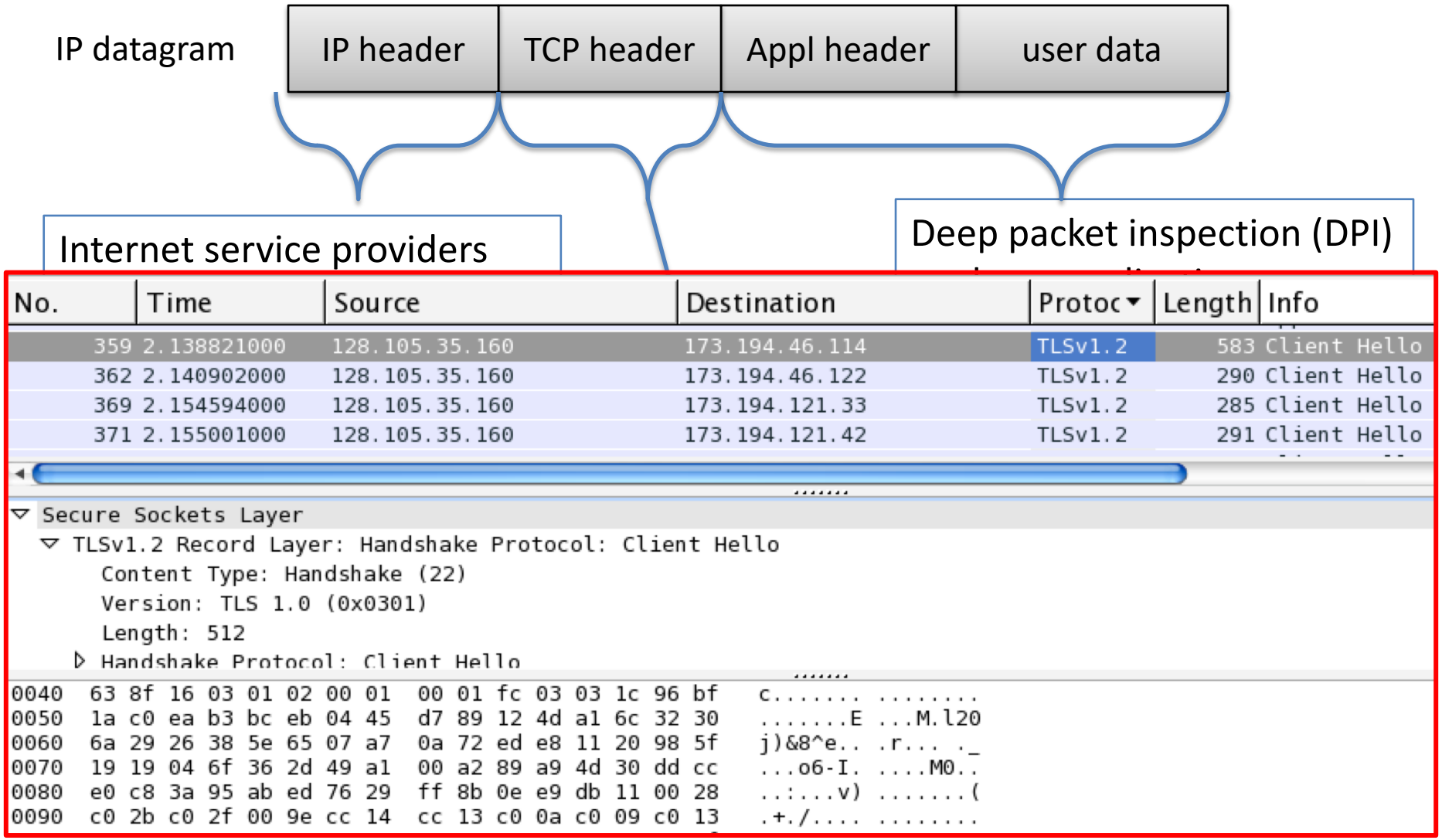


Large amounts of Internet traffic cross relatively few key points

Interception technology

- From Narus' website (http://narus.com/index.php/product/narusinsight-intercept):
  - "Target by phone number, URI, email account, user name, keyword, protocol, application and more"
  - "Service- and network agnostic"
  - "IPV 6 ready"
  - Collects at wire speeds beyond 10 Gbps

Types of packet inspection

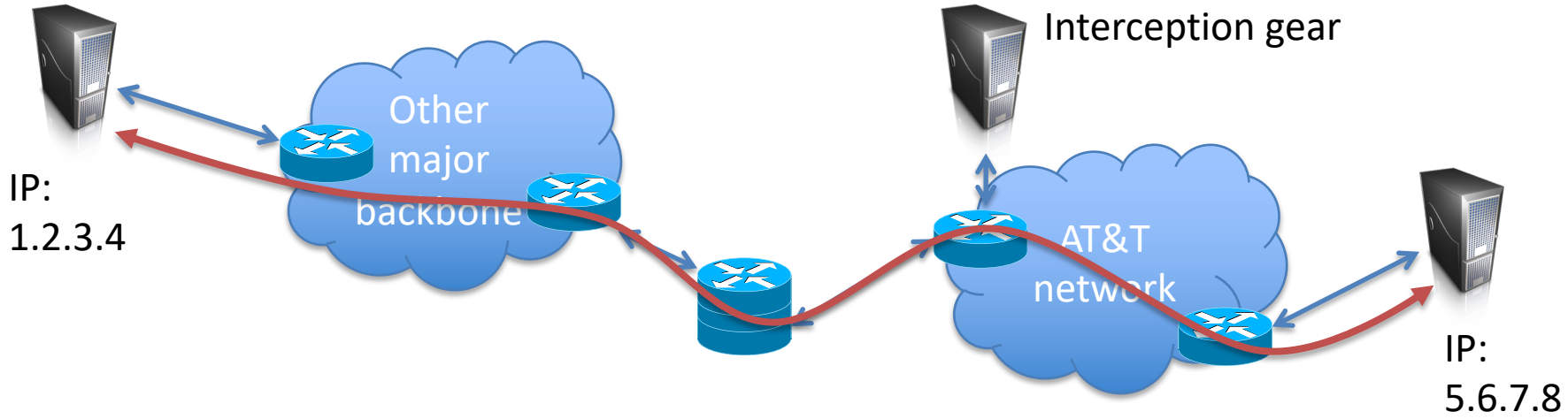


Lawful intercept in the United States

- CALEA
  - Communications Assistance for Law Enforcement Act (1995)
- FISA
  - Foreign Intelligence Surveillance Act (1978)
  - Demark boundaries of domestic vs. foreign intelligence gathering
  - Foreign Intelligence Surveillance Court (FISC) provides warrant oversight
    - Civil liberty groups criticize efficacy of oversight
- Also applies to data hosted by services (e.g., your Gmail)
- Most (almost all?) national governments mandate some kind of lawful intercept capabilities

Preventing intercept

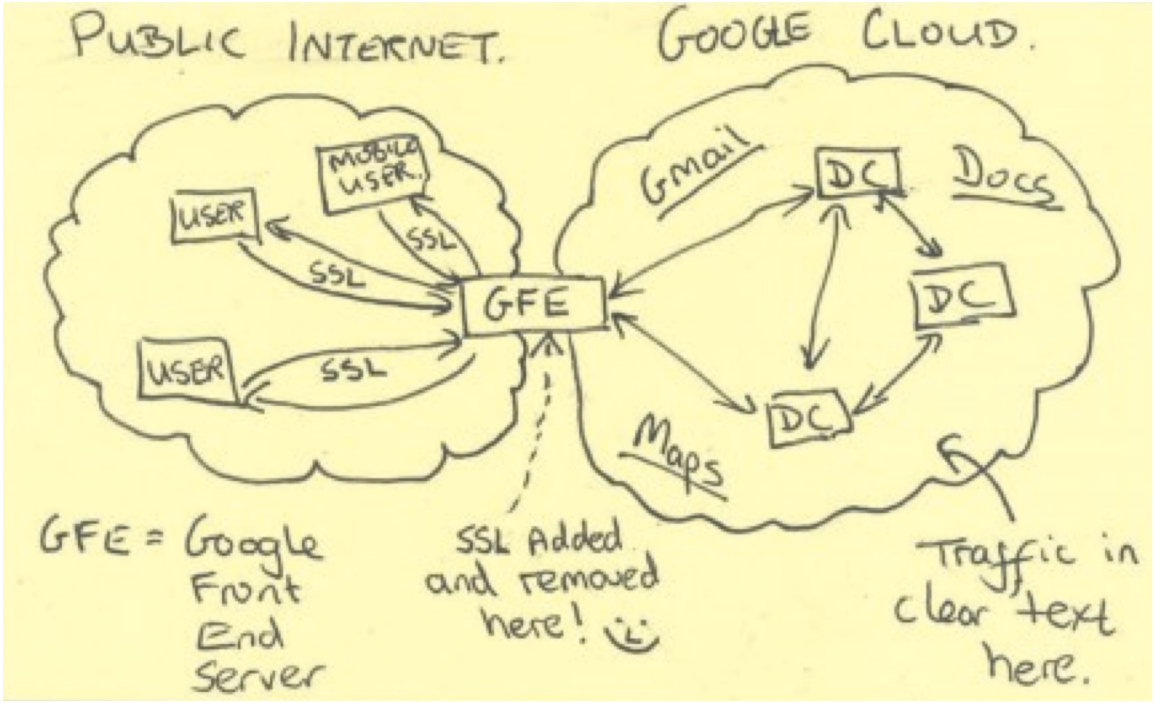
- End-to-end encryption (TLS, SSH)



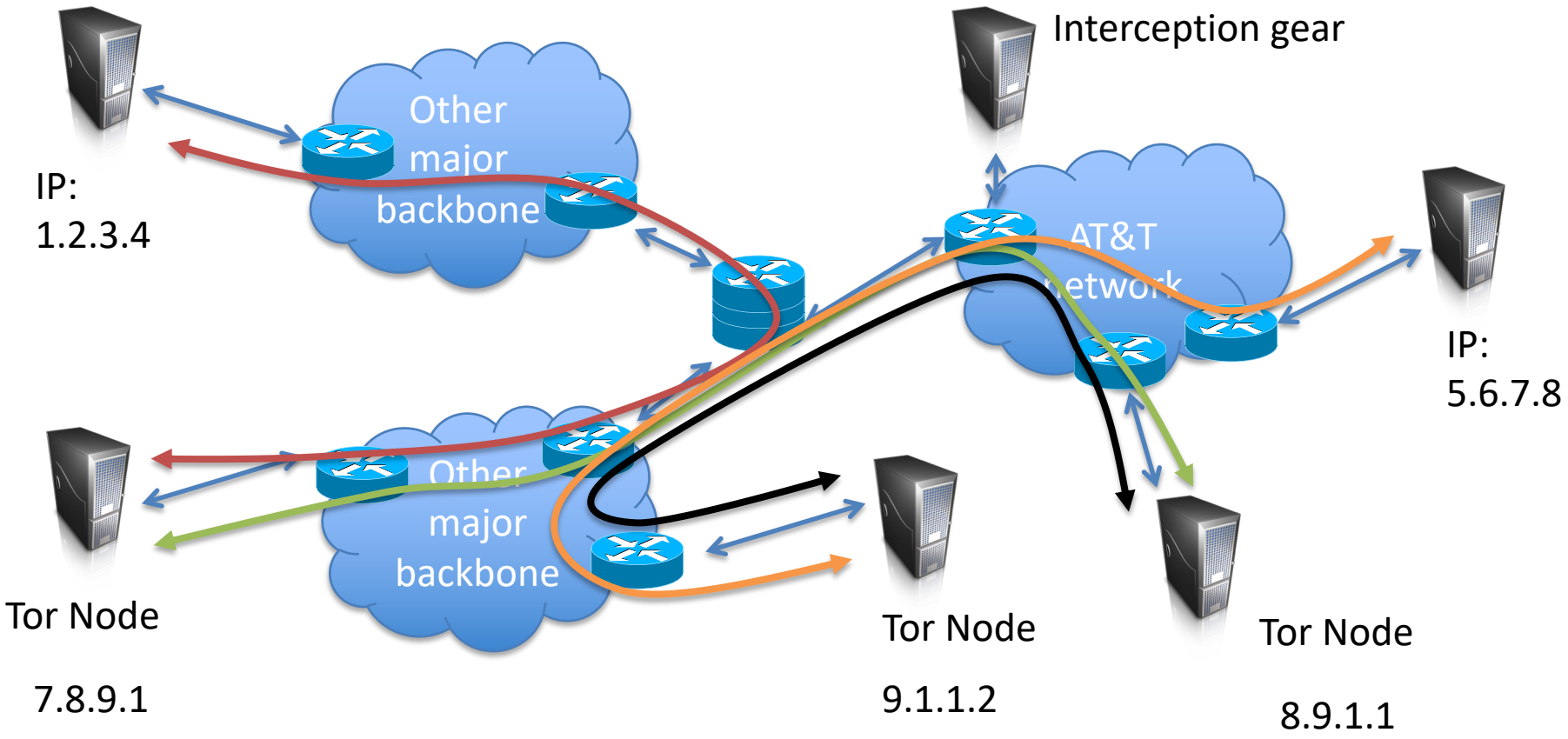
- What does this protect? What does it leak?
- What can go wrong?

End-run around HTTPS

- HTTPS terminated at edge of Google networks
- Internal data center-to-data center communications on privately leased lines
  - No encryption up until summer 2013



Tor (The Onion Router)



IP:
1.2.3.4

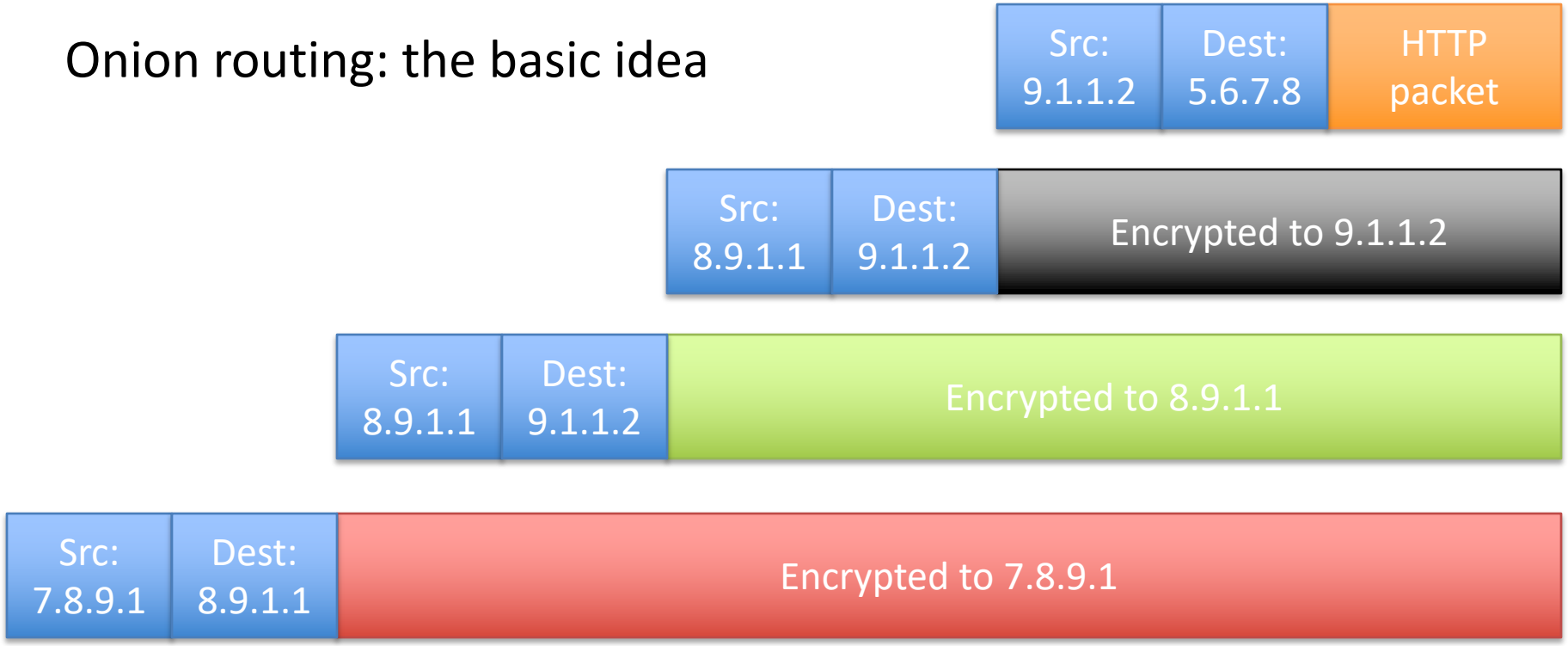
7.8.9.1

8.9.1.1

9.1.1.2

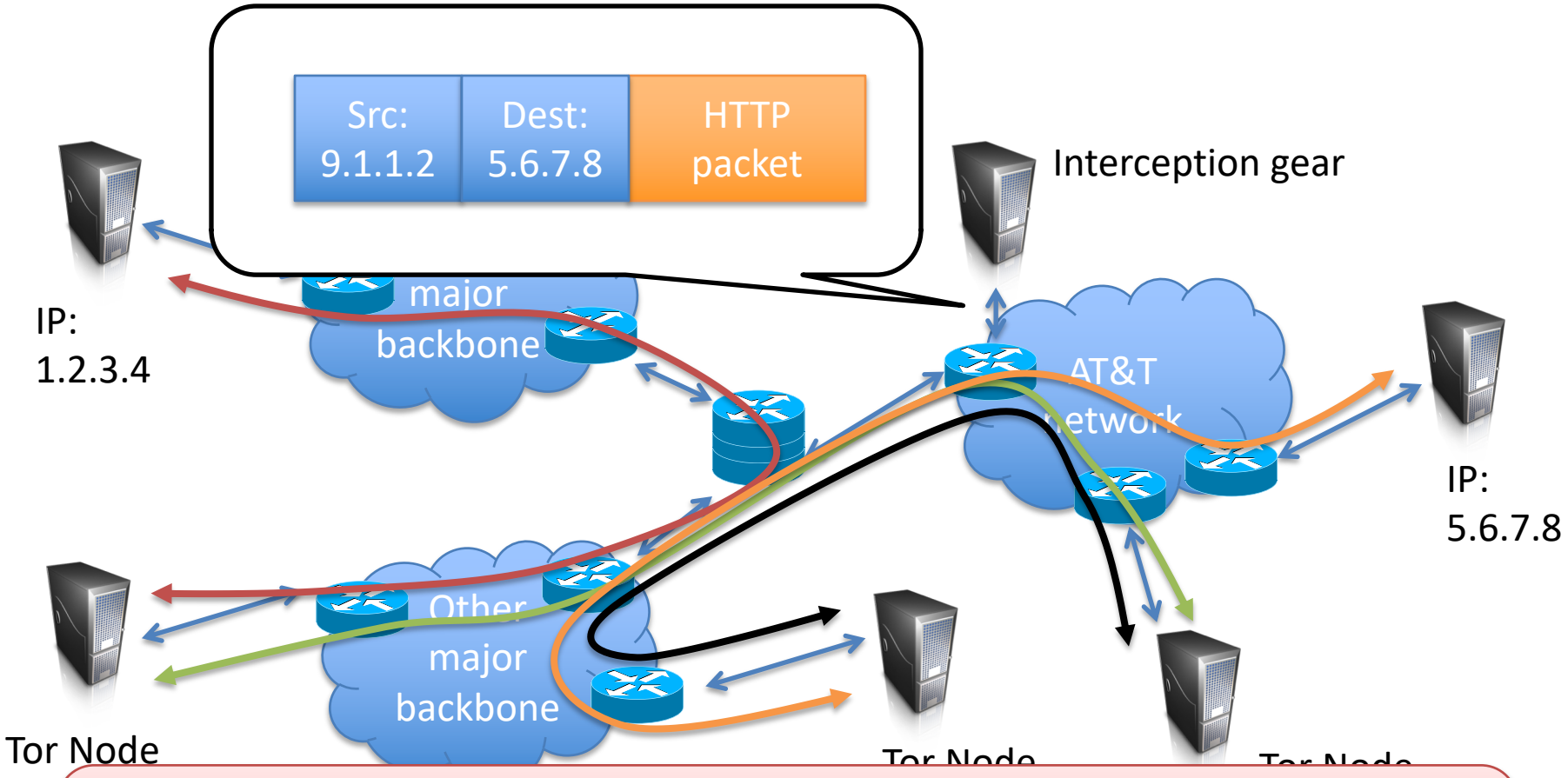
IP:
5.6.7.8

Onion routing: the basic idea



Tor implements more complex version of this basic idea

What does adversary see?



Tor obfuscates who talked to who, need end-to-end encryption (e.g., HTTPS) to protect payload

Tor onion services (aka hidden services)

Enable web servers to operate anonymously (hides IP address)

Beyond Silk Road 2.0, over 400 'dark web' Tor sites seized by FBI

Summary: *Hundreds of darknet websites have been identified and taken down -- and the Tor Project isn't sure how.*

Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE Monday, August 12, 2019

Four Men Sentenced to Prison for Engaging in a Child Exploitation Enterprise on the Tor Network

The “crypto wars”

- “Going dark” debate over last few years
  - Police and others argue encryption is preventing criminals, terrorists from being caught
  - Push for building in backdoors into crypto & other systems
  - Manhattan DA have interesting report about smartphone unlocking
- Long history
  - 1990s era export controls on cryptography
  - 1990s failed Clipper chip effort
- Consensus among cryptographers & security experts:
  - Mandated backdoors fundamentally weaken security
  - Keys under doormats report (https://www.schneier.com/academic/paperfiles/paper-keys-under-doormats-CSAIL.pdf)

Former FBI general counsel Jim Baker talking Thurs at 11:40am (B091)

Surreptitious backdoors: sabotaging TLS

- NIST's Dual EC pseudorandom number generator (PRNG) backdoored
  - Mandated public parameters are public key
- Intuitively:
  - TLS ClientHello random nonce is public-key encryption of values sufficient to derive session key

Schneier, Fredrikson, Kohno, Ristenpart.
Surreptitiously Weakening Cryptographic Systems
https://eprint.iacr.org/2015/097.pdf

Topics for today

- Mass surveillance
- The “going dark debate”
- Internet censorship
- Targeted espionage

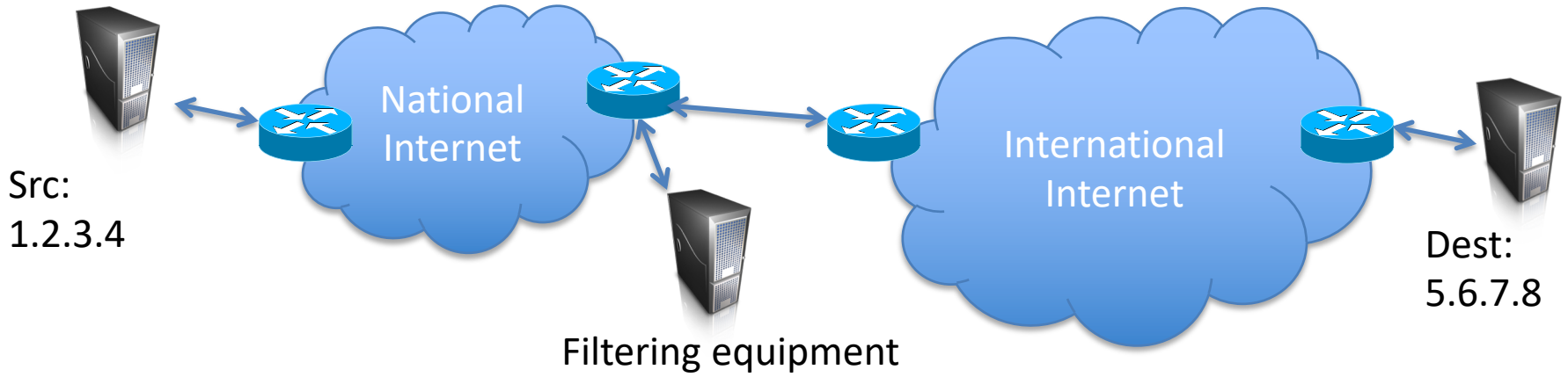
What happened in Iran last month?

LILY HAY NEWMAN SECURITY 11.17.2019 03:34 PM

How the Iranian Government Shut Off the Internet

After years of centralizing internet control, Iran pulled the plug on connectivity for nearly all of its citizens.

Censorship via Internet filtering

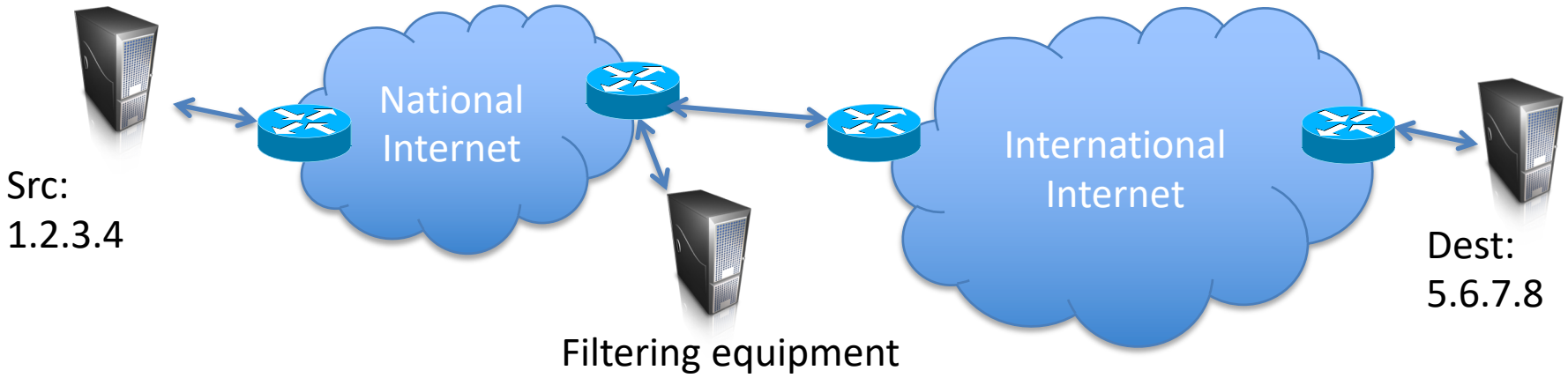


- Golden Shield Project (Great Firewall of China) most famous example
- But many other nations perform filtering as well including
  - Iran, Syria, Pakistan (YouTube anecdote)
  - Turkey (twitter ban)
  - Singapore, Australia (proposed legislation)
  - …

Security technologies power censorship

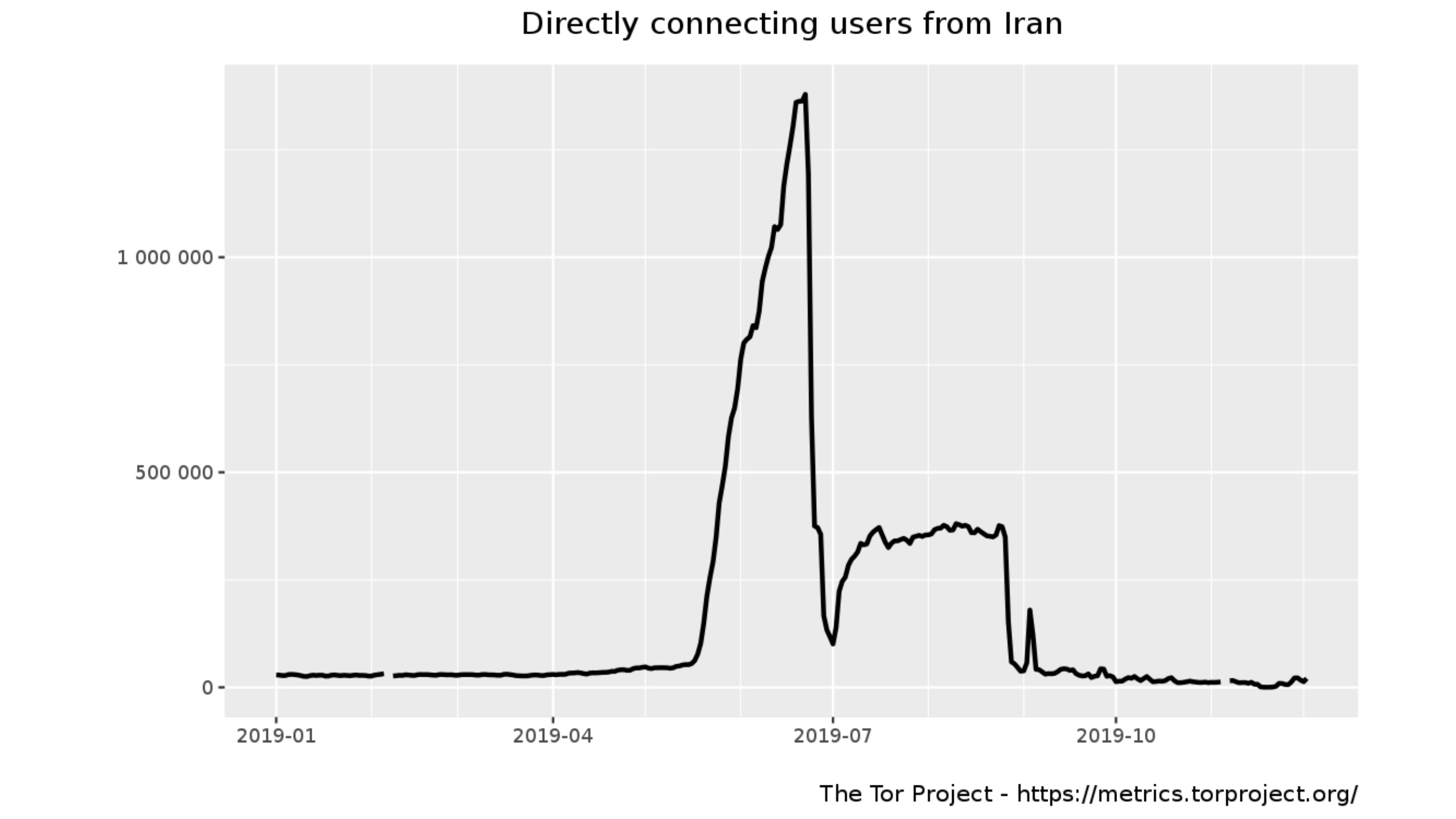
- Reports of products being used in Syria
  - Blue Coat (http://www.bluecoat.com/)
  - NetApp (http://www.netapp.com/)
- Iran, Saudi Arabia
  - Secure Computing's SmartFilter software
  - Secure Computing recently bought by McAffee
- Embargos prevent selling directly by USA companies, but resellers end up doing so

How would filtering work?



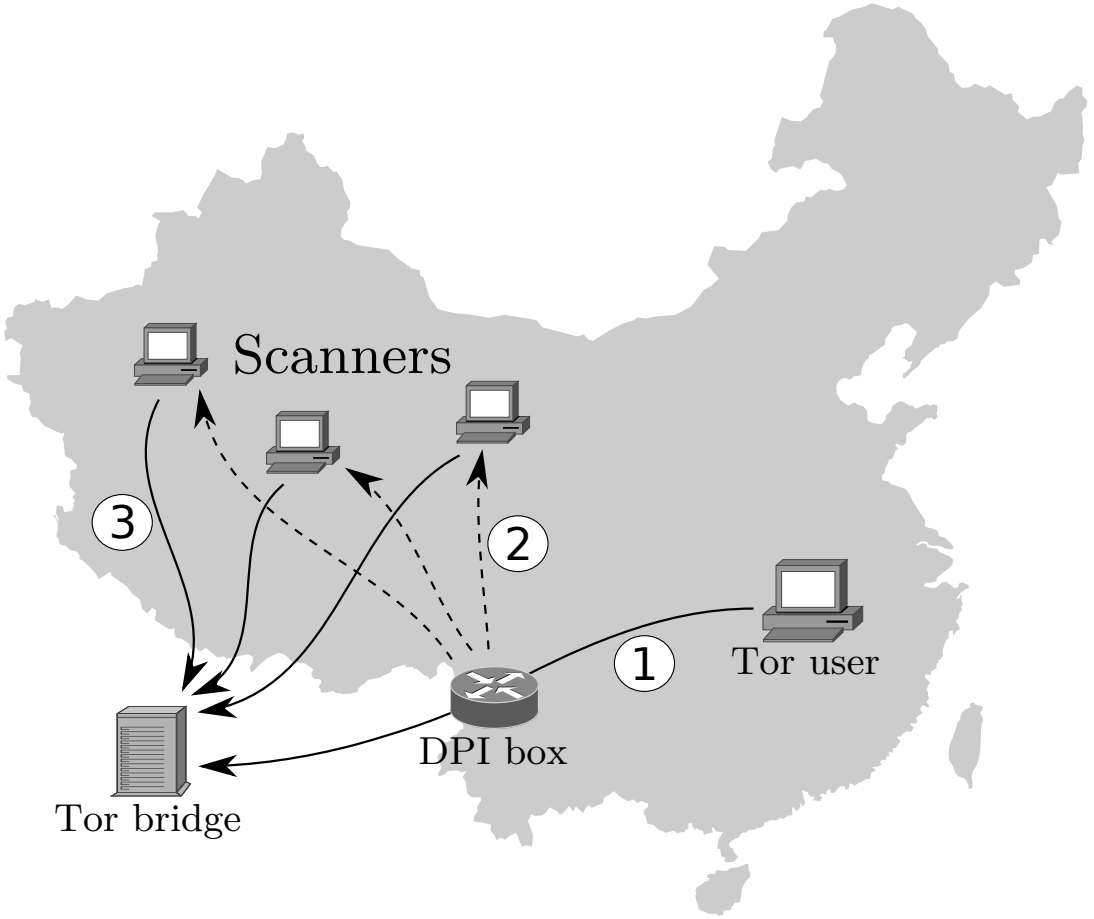
Islamic Republic of Iran

- Every ISP must run “content-control software”
  - SmartFilter (up until 2009)
  - Nokia Siemens DPI systems
- According to wikipedia Facebook, Myspace, Twitter, Youtube, Rapidshare, Wordpress, BBC, CNN, all have been filtered
- Occassional widespread filtering of Tor, TLS, other encrypted protocols


Directly connecting users from Iran
1 000 000
500 000
0
2019-01
2019-04
2019-07
2019-10
The Tor Project - https://metrics.torproject.org/

Golden Shield Project (Great Firewall of China)

- IP filtering
- DNS filtering / redirection
- URL filtering
- Packet filtering (search keywords in TCP packets)
  - Send TCP FIN both ways
- Protocol filtering
  - Tor is mostly shut down



From [Winter, Lindskog 2012]

Topics for today

- Mass surveillance
- The “going dark debate”
- Internet censorship
- Targeted espionage

Targeted attacks

- Dissidents, journalists, activists targeted by nation-states
  - Phishing attacks, botnet-style C&C servers to collect data
  - Remote Access Trojans (RATs)
- Small industry of companies providing “lawful access” tools


From: Melissa Chan <melissa.aljazeera@gmail.com>
To:
Sent: Tuesday, 8 May 2012, 8:52
Subject: Torture reports on Nabeel Rajab

Acting president Zainab Al Khawaja for Human Rights Bahrain reports of torture on Mr. Nabeel Rajab after his recent arrest.

Please check the attached detailed report along with torture images.

1 attachment: Rajab.rar 1.4 MB Save

Figure 1: E-mail containing FinSpy.

https://www.usenix.org/system/files/conference/usenixsecurity14/sec14-paper-blond.pdf
https://www.usenix.org/system/files/conference/usenixsecurity14/sec14-paper-marczak.pdf
https://www.usenix.org/system/files/conference/usenixsecurity14/sec14-paper-hardy.pdf

Tracking GhostNet (2009)

http://www.nartv.org/mirror/ghostnet.pdf

- In-depth investigation into espionage campaign against Tibetan community
- Discovered malware operating on Tibetan assets
- Reverse engineered, found C&C servers
  - No authentication to access C&C servers
  - Lists all computers infected by malware
- 1,295 infected computers in 103 countries
  - 26.7% government- or politics-related

2009 Operation Aurora

- Elderwood advanced persistent threat group (alleged ties to PLA)
  - "Waterhole attacks" (compromise site target company's employees visit)
- Targeted systems at Google (IP theft, Gmail accounts of Chinese dissidents), Adobe, Juniper, Rackspace, Microsoft, …
- One theory: alleged counterespionage campaign
  - Figure out what Gmail accounts being monitored by US Government
  - Remember: CALEA/FISA lawful intercept

Topics for today

- Mass surveillance
- The “going dark debate”
- Internet censorship
- Targeted espionage