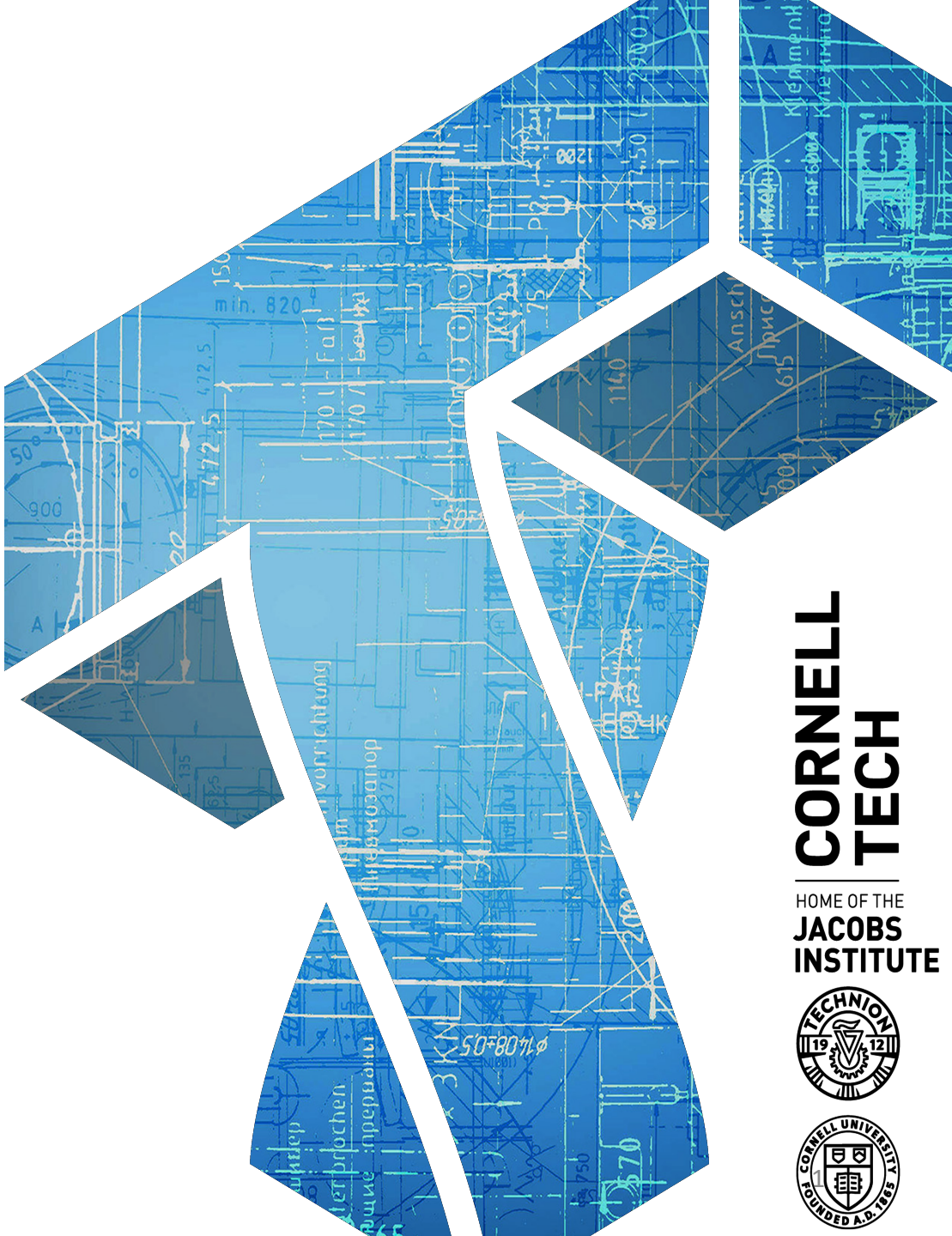
CS 6431: Anonymity

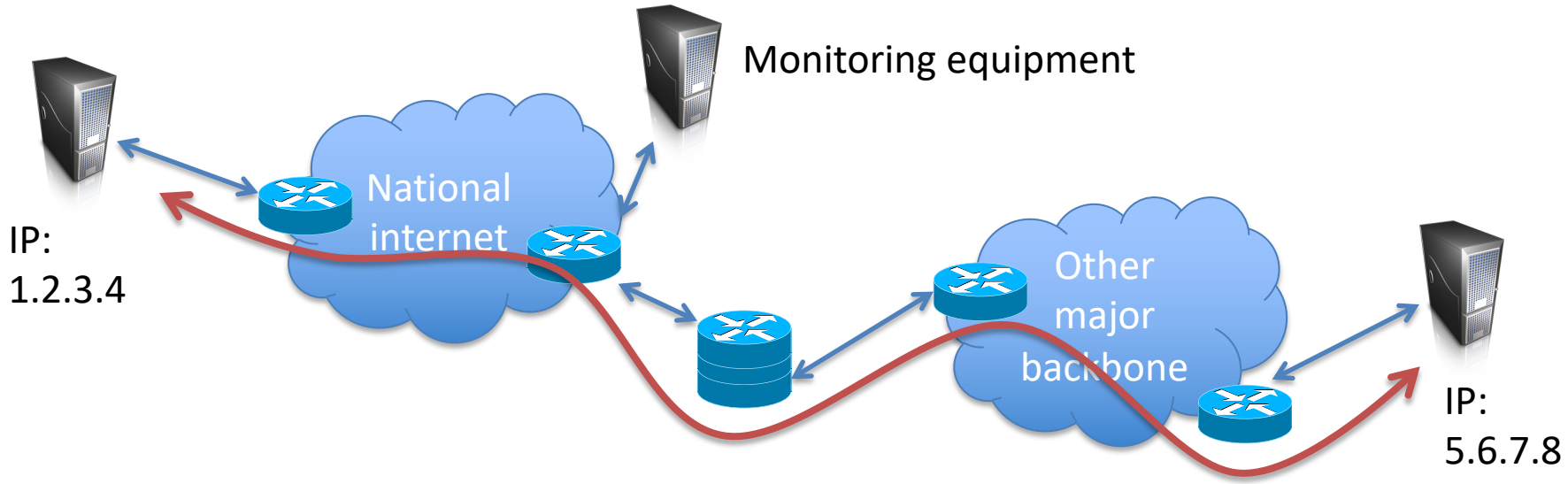
Instructor: Tom Ristenpart

https://github.com/tomrist/cs6431-fall2021



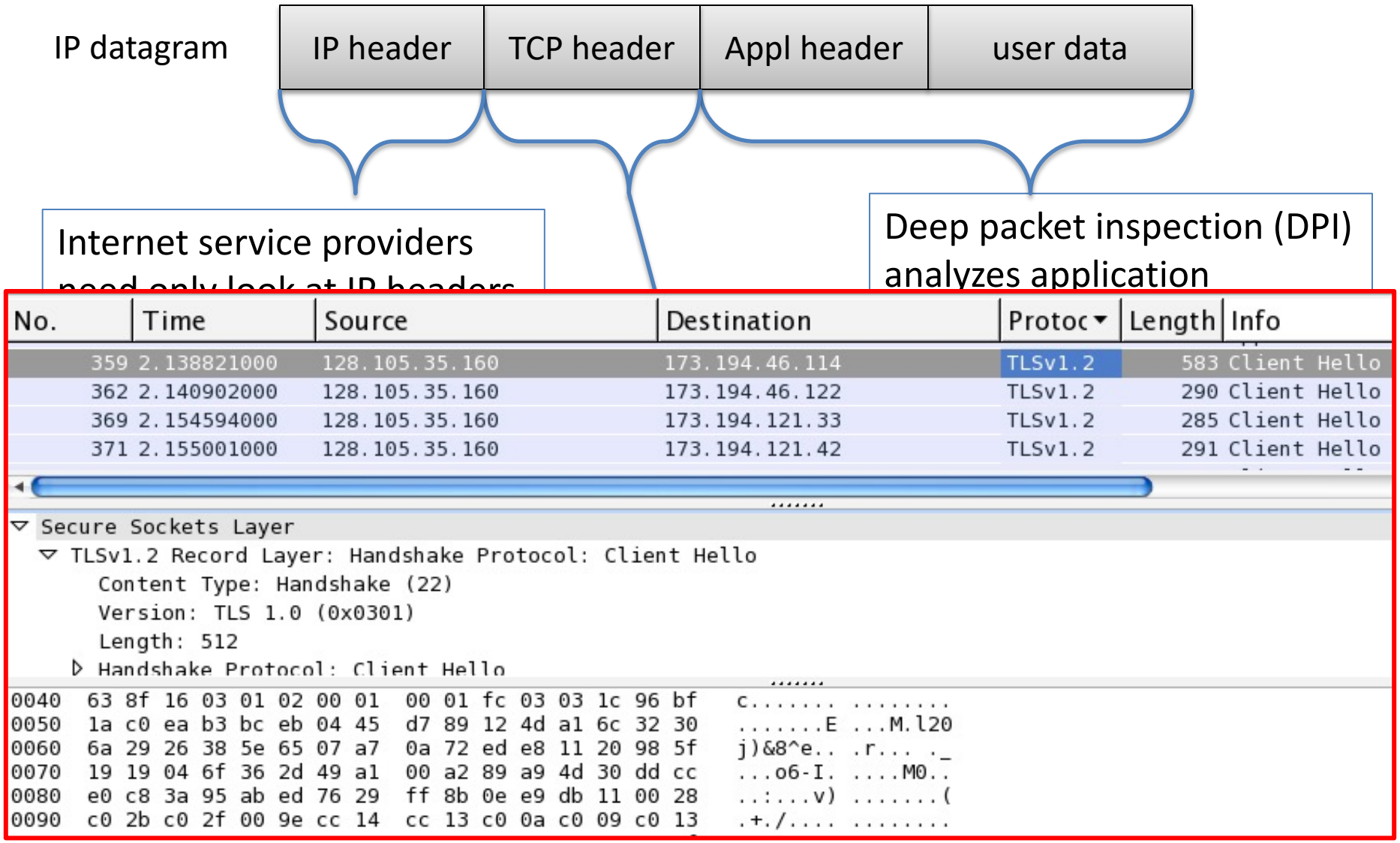
CORNELL TECH
HOME OF THE JACOBS INSTITUTE

Internet and identification



- IPv4 (and IPv6) reveal metadata:
  - IP addresses of source, destination
  - Port of destination
- End-point threat model
  - Servers log who accesses them
- Network threat model
  - ISPs / nation-states monitor/intercept traffic

Types of packet inspection



DPI technology and state use

- AT&T whistleblower alleged Narus equipment used by US NSA in San Francisco AT&T office (2006)

- From Narus' website (now defunct) (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

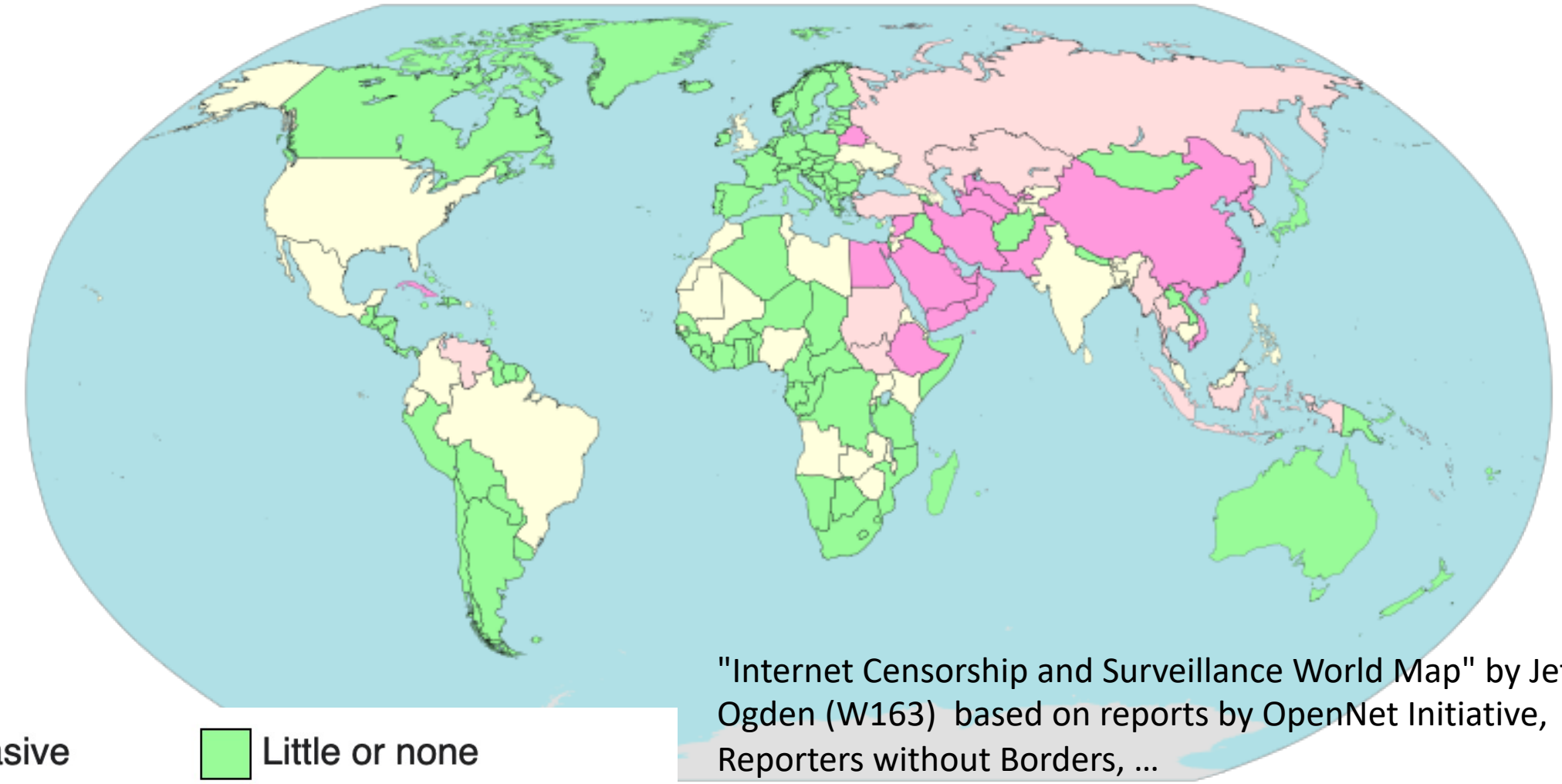
DPI technology and state use

- Turk Telecom & Telecom Egypt using Sandvine/Procera DPI boxes
- “Targeted users in Turkey and Syria who downloaded Windows applications from official vendor websites including Avast Antivirus, CCleaner, Opera, and 7-Zip were silently redirected to malicious versions by way of injected HTTP redirects.”
  - https://citizenlab.ca/2018/03/bad-traffic-sandvines-packetlogic-devices-deploy-government-spyware-turkey-syria/

DPI technology and state use

- Internet censorship refers to government blocking of content
  - Great Firewall of China (Golden Shield)
  - Iranian censorship apparatus
  - United States, UK, Singapore, India, …
- https://tools.ietf.org/id/draft-irtf-pearg-censorship-03.html

Current estimates of Internet surveillance & censorship



"Internet Censorship and Surveillance World Map" by Jeffrey Ogden (W163) based on reports by OpenNet Initiative, Reporters without Borders, …

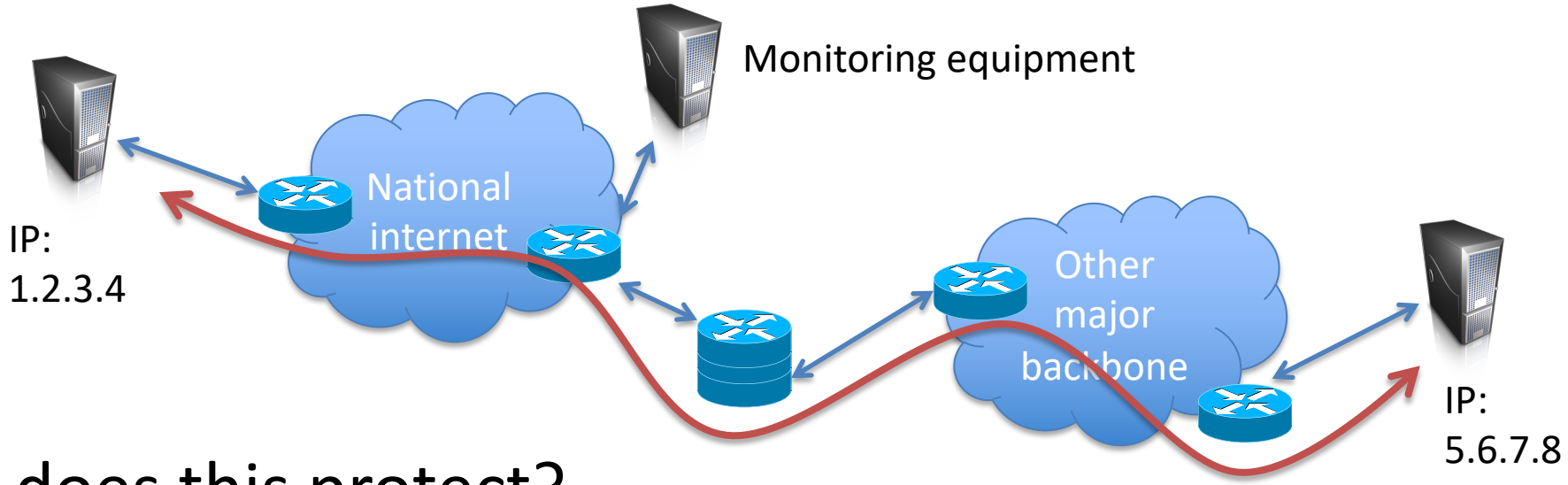
Magenta-colored countries are countries with pervasive censorship and surveillance of the Internet

Discussion: how to frame monitoring/censorship

- Is (all) monitoring/censorship bad?
- Should governments regulate internet content?
- What are pitfalls of building circumvention tools?

Preventing monitoring/intercept

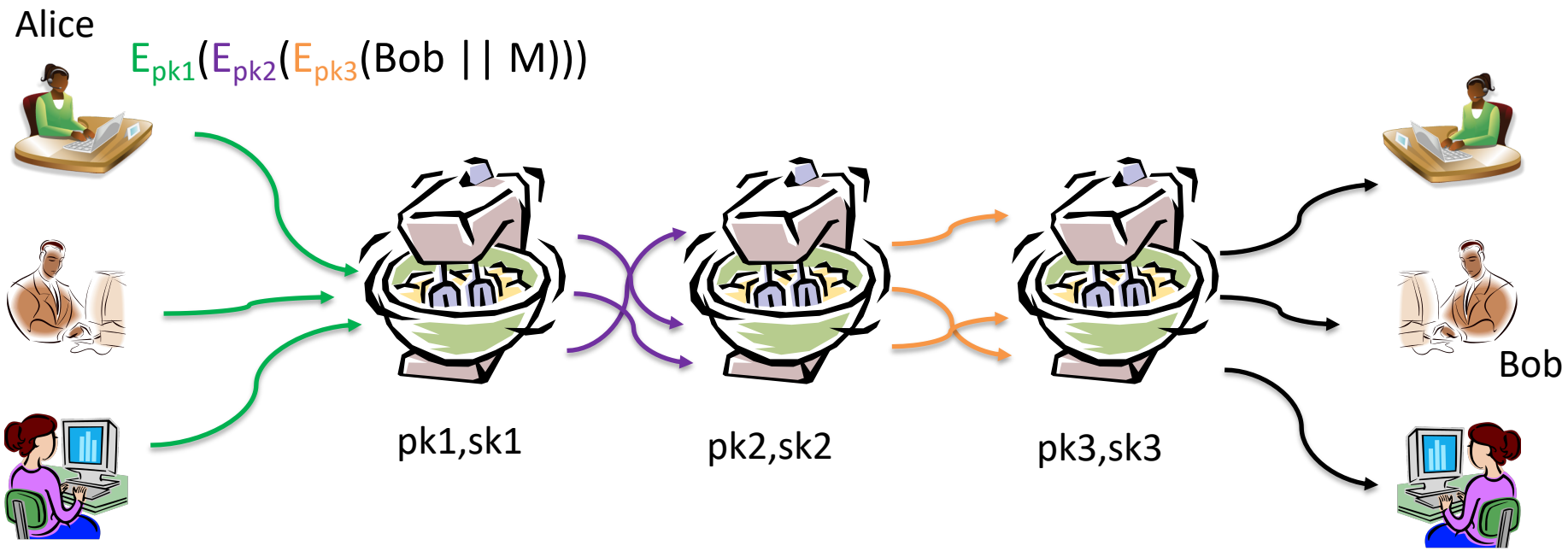
- End-to-end encryption (HTTPS, SSH)



- What does this protect?
- What does it leak?

Onion routing: history

- Chaum's 1981 mix-net design
  - Wrap messages in layers of public-key encryption, and relay through network of "mixes" that decrypt, delay, and re-order messages



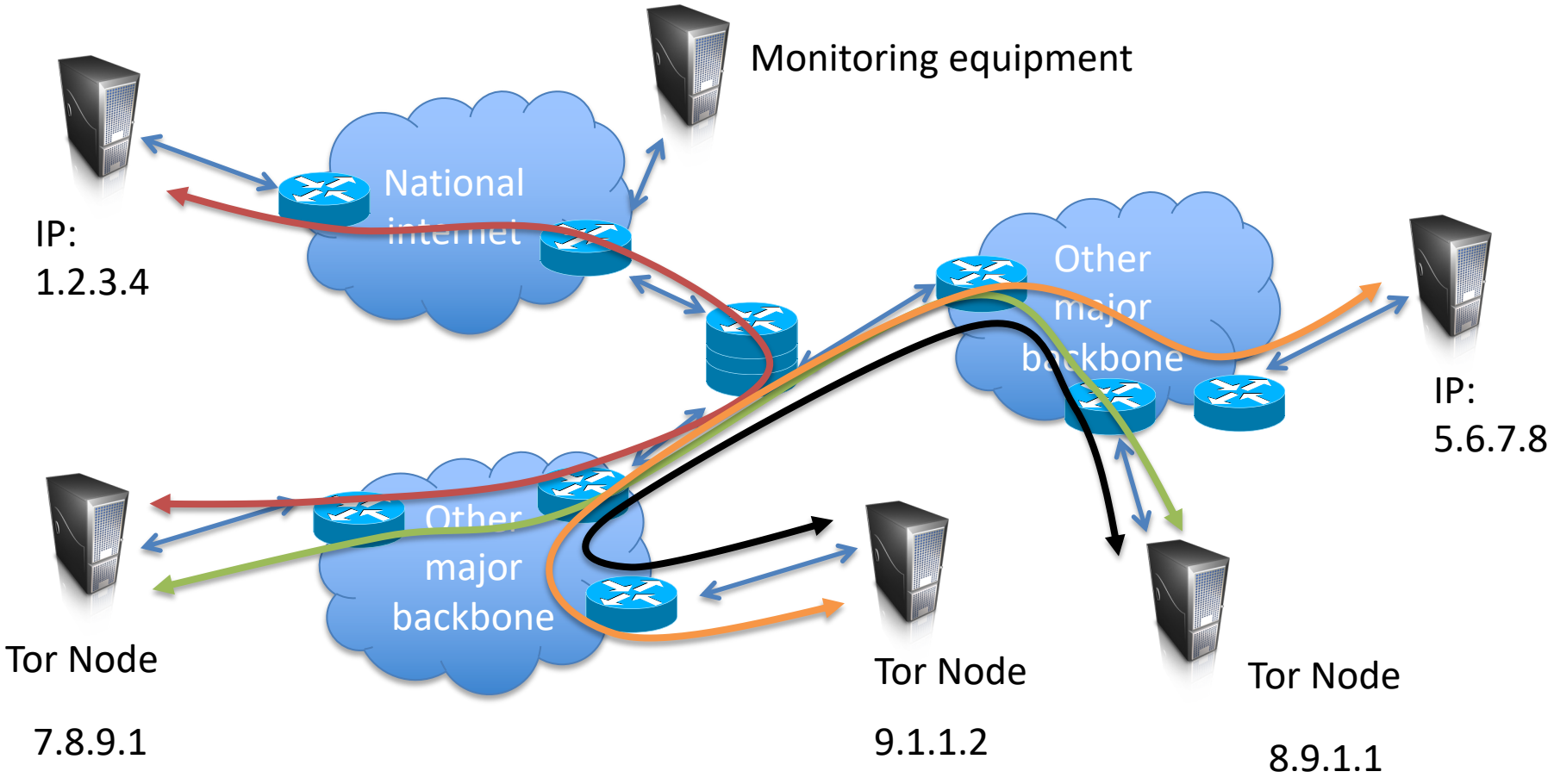
Onion routing: history

- Chaum's 1981 mix-net design
  - Wrap messages in layers of public-key encryption, and relay through network of "mixes" that decrypt, delay, and re-order messages
  - High-latency design (delays messages). Maybe suitable for email
    - Examples: Mixminion, Babel, Mixmaster
- Low-latency designs (interactive traffic)
  - Mostly gives up on:
    - end-to-end traffic analysis attacks
    - active watermarking attacks

Tor (The Onion Router)

- Second generation onion router system
  - Built off previous designs put forth in the Onion Routing project
  - Bunch of research papers looking at anonymity systems
  - Anonymizing TCP/IP traffic from clients (web browser)
  - Hidden services
- Garnered test-of-time award USENIX Security 2014
- Deployed to significant impact
  - One author went to found Tor Project
  - ~6500 volunteer-provided onion relays
  - >2 million daily users
  - 250 Gbit/s bandwidth usage

Tor (The Onion Router)



IP: 1.2.3.4

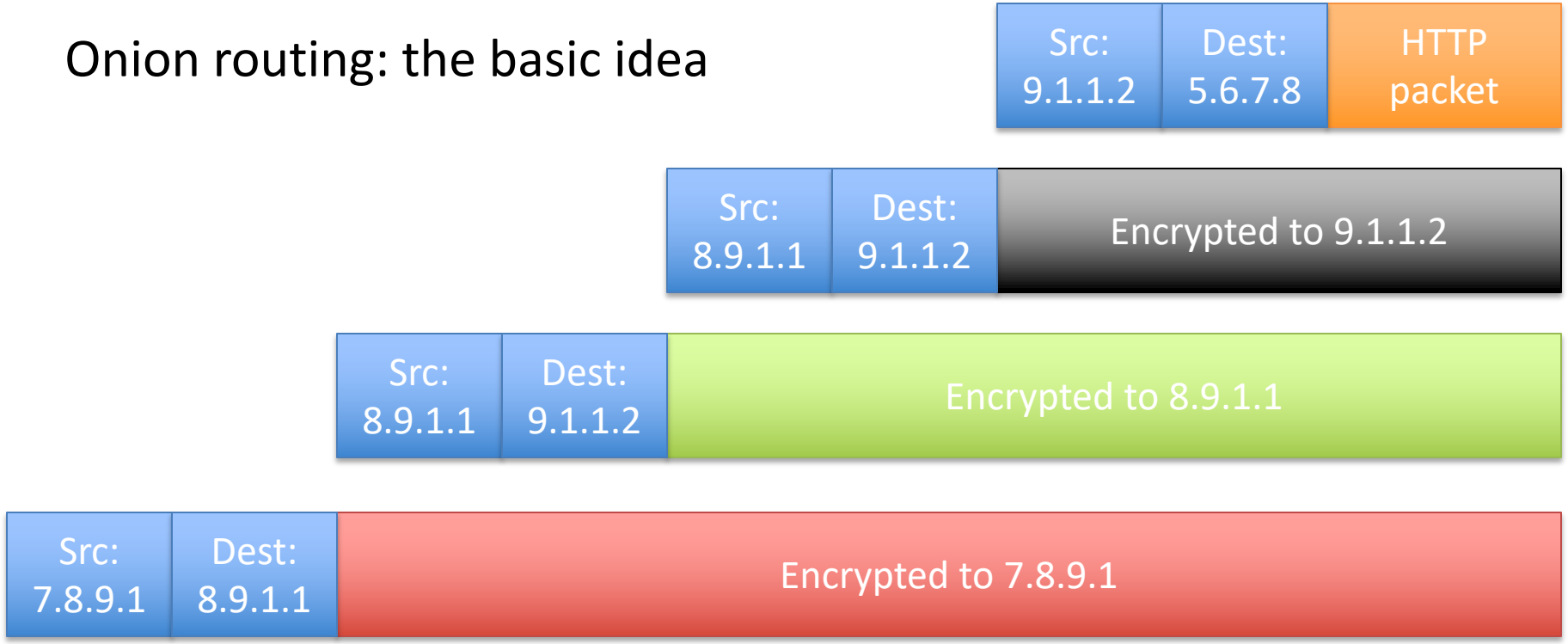
7.8.9.1

8.9.1.1

9.1.1.2

IP: 5.6.7.8

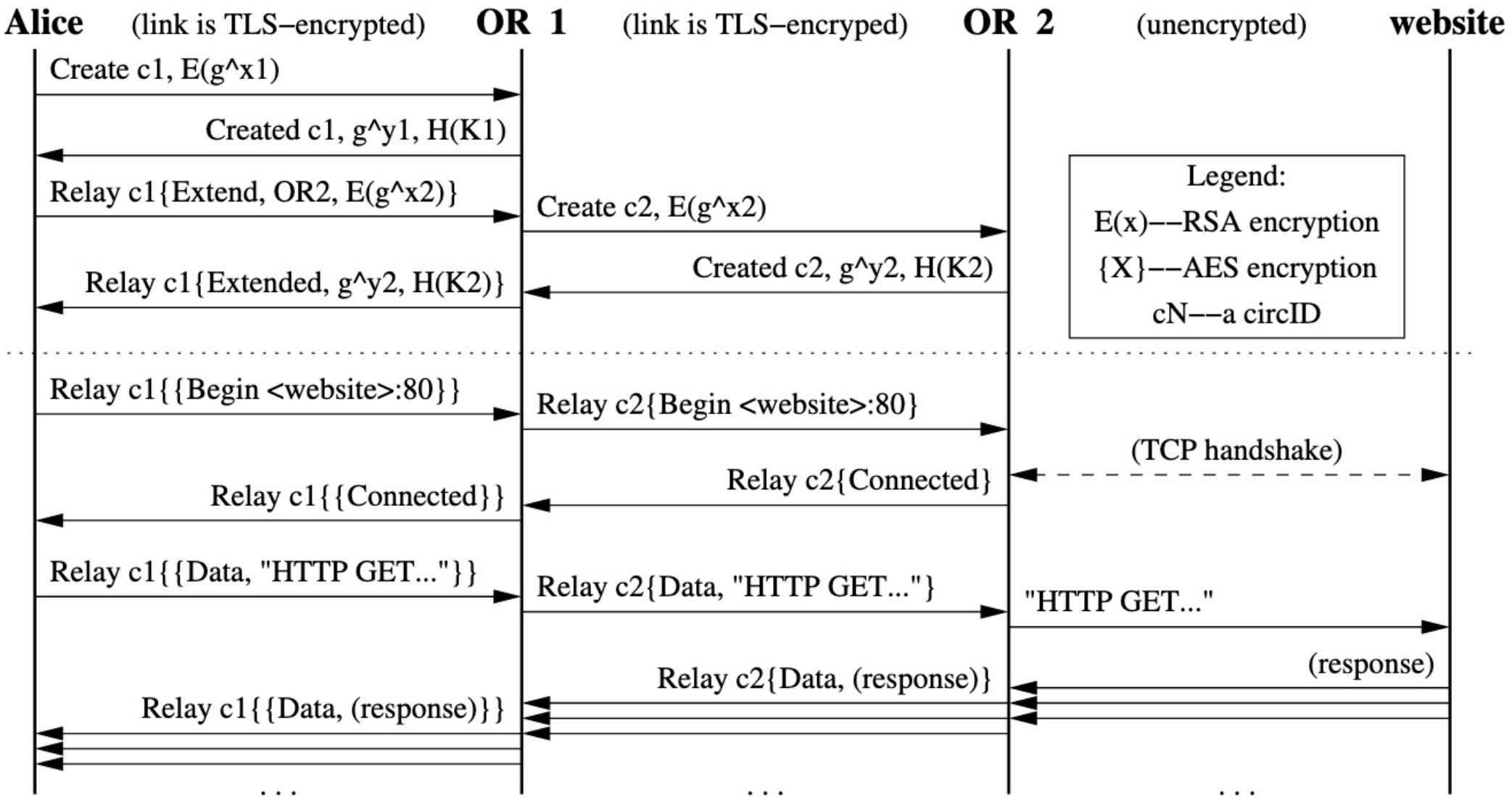
Onion routing: the basic idea



Tor implements more complex version of this basic idea

All data tunneled over point-to-point TLS connections

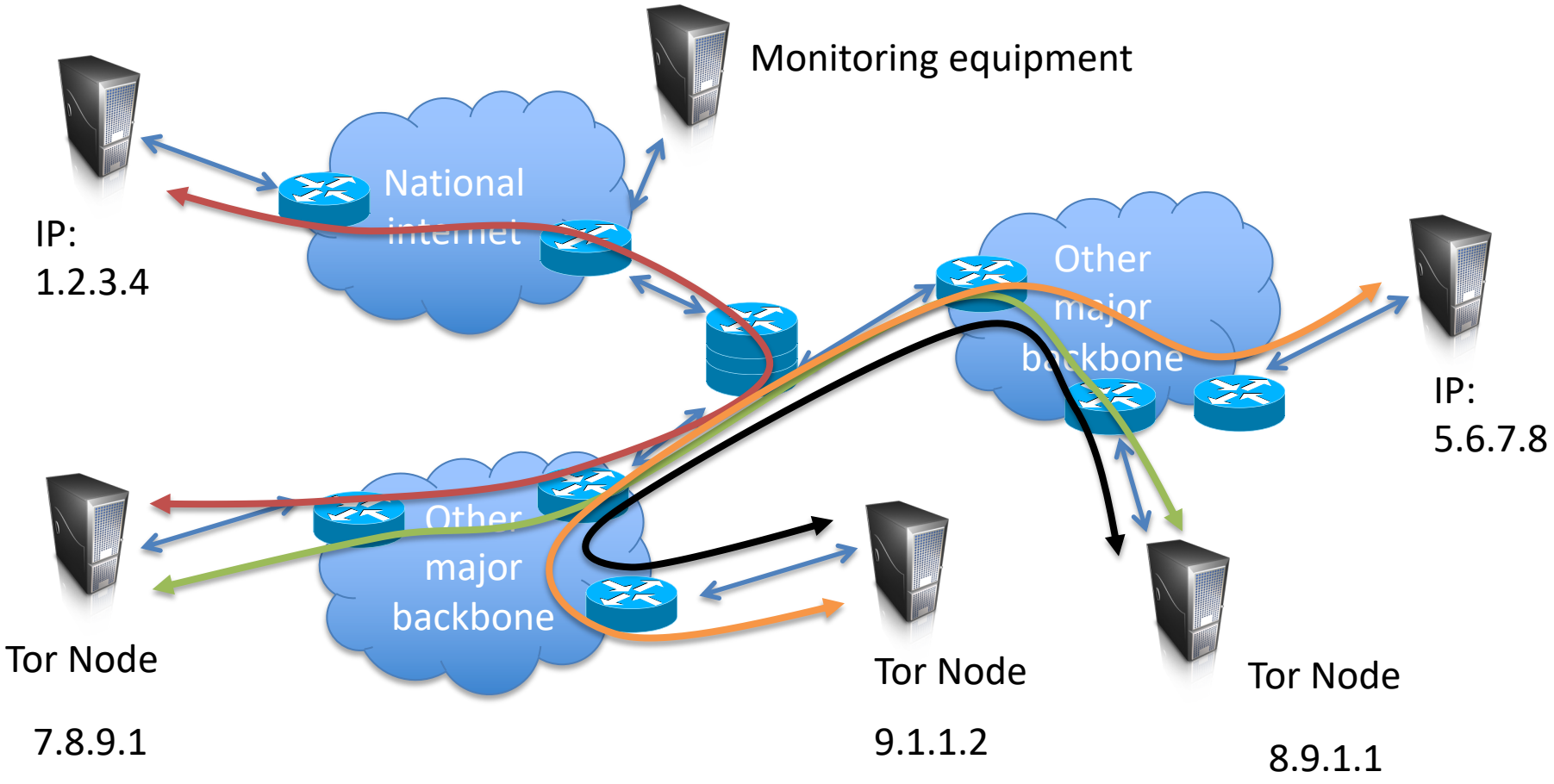
Circuit construction



Design considerations

- How to know about onion router nodes?
  - Directory service: small group of nodes that manage list of nodes and their public keys
- Node selection policies
- Integrity checksums (message authentication)
- Rate limiting and fairness
  - Denial-of-service attacks
- Exit policies and abuse

Attacks / security issues?



Rendezvous points and hidden services

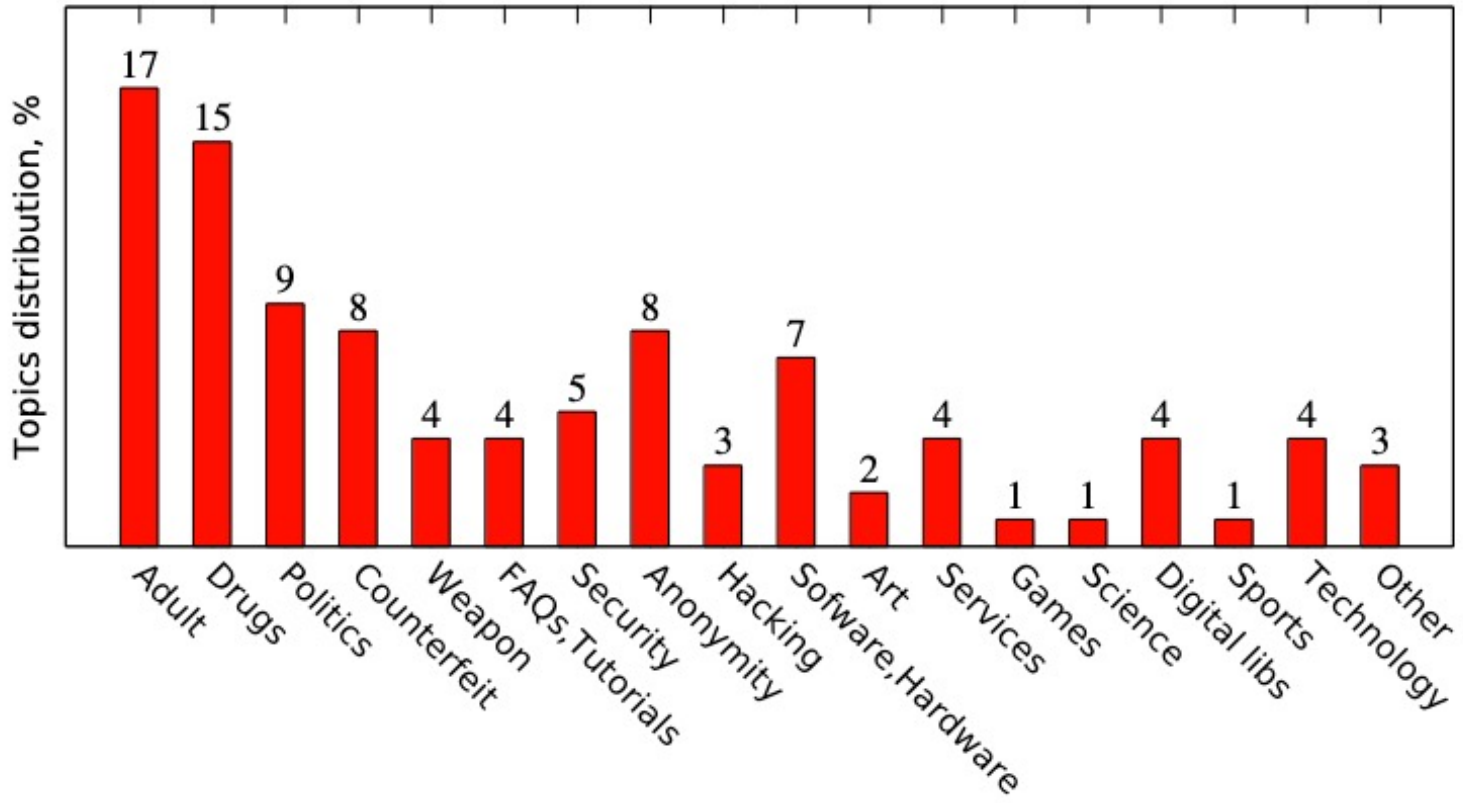
- So far client must know destination IP address
  - Client IP address hidden from endpoint
- What if we want to hide the server IP address from clients?
- Server picks some nodes as rendezvous points (RPs)
  - Advertise these nodes elsewhere (on the web)
  - Server builds circuit to each RP
  - Client builds circuit to a chosen RP
  - Perform end-to-end Diffie-Hellman key exchange through RP
- RP doesn’t know IP of either client or sender

Measurement studies of Tor?

- Shining Lights in Dark Places
  - "The large amount of exit bandwidth that we provided caused us to receive a large number of complaints ranging from DMCA §512 notices related to allegations of copyright infringement, reported hacking attempts, IRC bot network controls, and web page defacement. However, an enormous amount of malicious client activity was likely unreported."
  - http://damonmccoy.com/papers/PETS2008_37.pdf

Measurement studies of Tor?

- Hidden service crawling
  - [Biryukov et al. 2014]



Large literature on anonymity

- Design of anonymity systems
- Formal analysis
- Experimental analysis (attacks)
- Empirical measurement
- PETS (Privacy Enhancing Technology Symposium) venue has lots of anonymity related content