Technological Dystopias

Who am I

Questions

Why they are important?

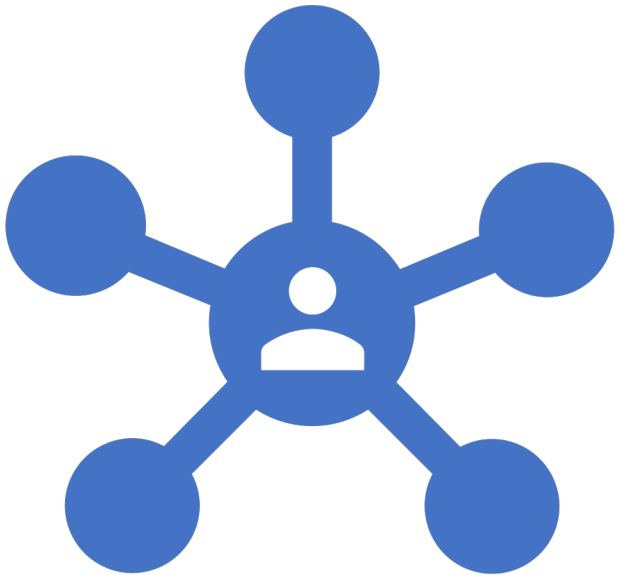
Knowledge

Understanding

Change

When to ask questions?

11/5/2019
Happy Fifth of November



What is **Technological Dystopia**

- An association between **technology** and catastrophic changes and a contaminated humanness that compromises social intercourse.


Let’s talk about
data collection

How much do you really pay for services?

- Free services aren’t free
- Your data is worth something
- Often the price is more expensive than if you were to pay for it
- Making the board of directors happy
- Consolidated servers
  - Ex. Google services, gmail, search, etc
  - Ex. Amazon prime, aws***, etc
  - Ex. Facebook, whatsapp, instagram

Kinds of data collected

- What info is on a smartphone?
  - Geolocation
  - Browser history
  - Purchases
  - Friends
  - WiFi points
  - Passwords
  - Credit card info
  - Misc PII
  - Communication

More Obscure tracking

- Photo location metadata
- Secret screen recording
- Microphone
- Browser tracking beacons
- Phone sensors
  - The accelerometer
  - Gyroscope
  - Magnetometer
  - GPS
  - Other small sensors
    - like the proximity sensor to detect when your phone is by your ear, or the ambient light sensor for auto-brightness.

Google and alexa

Always on

China’s Social Credit System

Prepare for some busy slides

Don’t worry… I’m not going to read them..

They’re just for your reference

China's Social Credit System

- China's "social credit system"
  - Rewards or punishments based on known and unknown inputs
    - Known inputs
      - Brower search
      - Facial recognition at protests
      - Bills not paid on time
  - Transportation – banned from flights, trains, and eventually busses
    - Low scores are even banned from domestic flights
    - Business class restrictions are first on trains
  - Throttling Internet speeds
  - Banning you and your children from the best schools
  - Banning you from the best jobs
  - Keeping you out of the best hotels
    - Common for refusing military service
  - Getting your dog taken away
    - Pet licenses can be revoked and pets confiscated
  - Being named as a "bad citizen" on public website
  - Etc...

Could social credit be a thing in US?

- How much do you pay for health/auto/etc insurance?
  - Lower payments by having an app or device plugged into car?
  - Age, gender, social and economic status, address, etc.
  - Life choices such as smoking, exercise, weight, etc?
  - Other public information such as driving records, bankruptcy filings, court documents, liens and evictions.
- Uber and AirBnB scores
  - If your ranking is significantly below average you can be banned by these apps.
- WhatsApp
  - Banned if too many users block you
- Content takedown
- How much does a person pay for a flight?
  - Browser Cookies, location, etc

What's the problem with that?

- Crimes are punished outside the legal system
  - no presumption of innocence
  - no legal representation
  - no judge
  - no jury
  - and often no appeal
  - In other words, it's an alternative legal system where the accused have fewer rights.
- Free speech concerns**

What's the problem with that?

- What is a right and what is a utility?
- Social media platforms are the modern "town square,"
  - A place where everyone comes to discover and share information and weigh-in with opinions.
  - Should everyone, regardless of their politics, class, or creed, have access to this marketplace of ideas?

EULA – End User License Agreement

- Do you have a choice?
- Can you redline contract?
- Do you read?

Threat scores

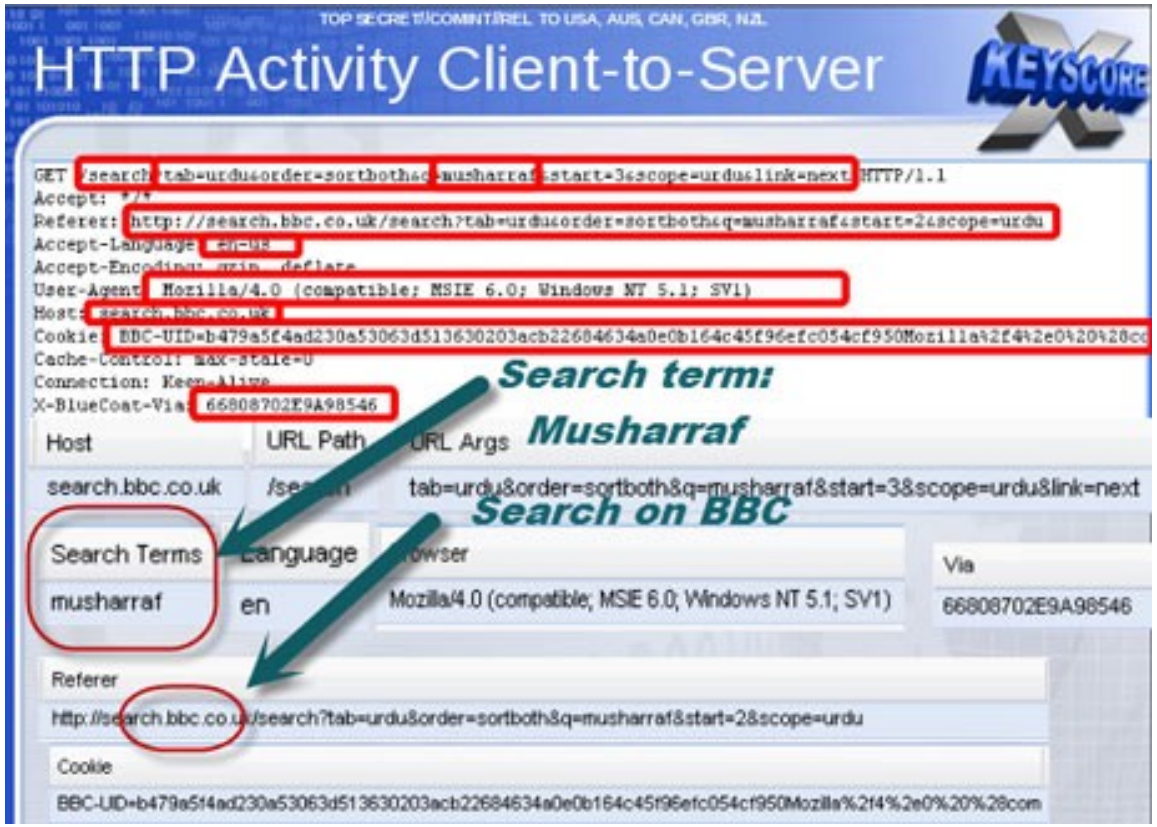
Face	Body	Police
Face recognition	Body movement recognition	Police Determined Threat score

Does anyone know who this is?

Hero or traitor?

NSA Programs

Xkeyscore



1. If you know the particular website the target visits. For this example, I'm looking for everyone in Sweden that visits a particular extremist web forum.

Scroll down to enter a country code (Sweden is selected

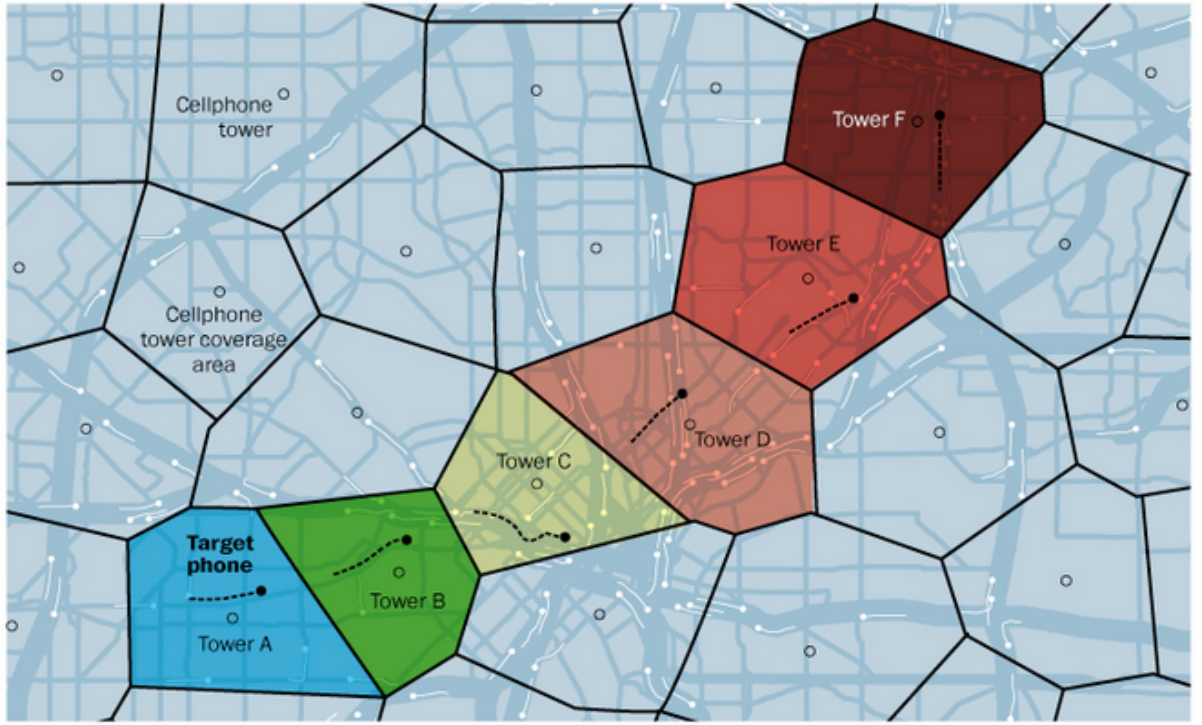
The website URL (aka "host) is entered in with a wildcard to account for "www" and "mail" other hosts.

To comply with USSID-18 you must AND that with some other information like an IP or country

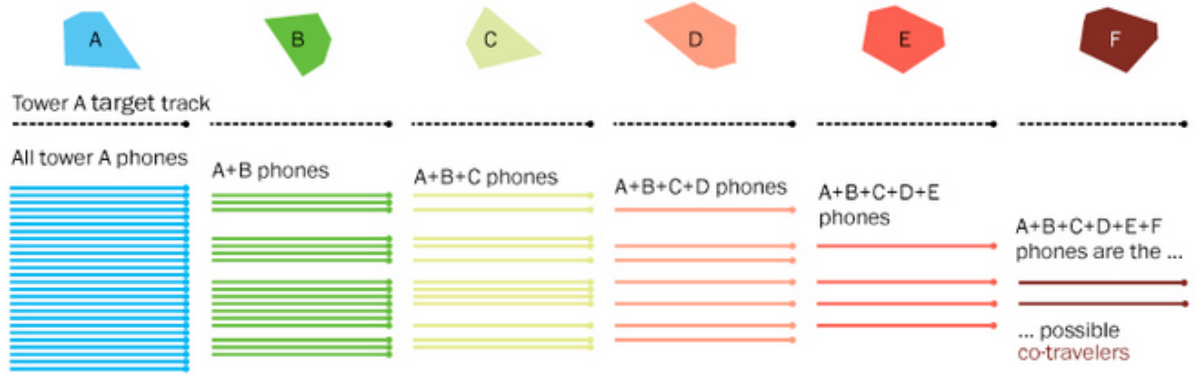
NSA Programs

FASCIA

By tracking all phones within a cell tower area along with the target phone, co-travelers can be isolated.



As the target phone moves from tower to tower, fewer and fewer potential co-travelers remain.

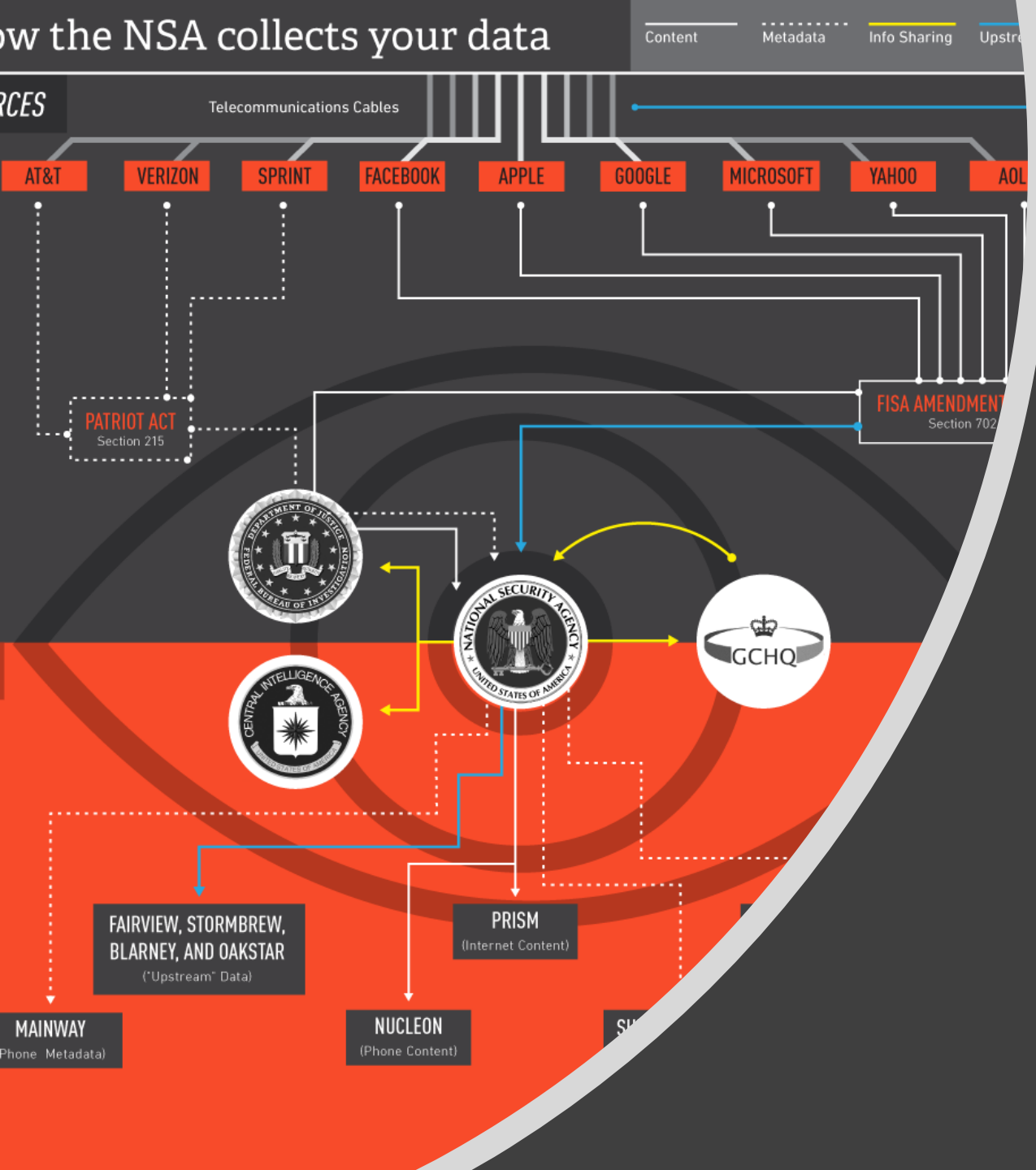


NSA Programs

- **Optic Nerve**
  - Webcam conversations
- **Boundless Informant**
  - Metadata
  - Huge repository
  - Why metadata is important
- **DishFire**
  - Cell phones to view financial transactions, monitor border crossings, and meetings between unsavory characters.
- **PRISM**
  - PRISM is a code name for a program under which the United States National Security Agency collects internet communications from various U.S. internet companies. The program is also known by the SIGAD US-984XN.

NSA Programs

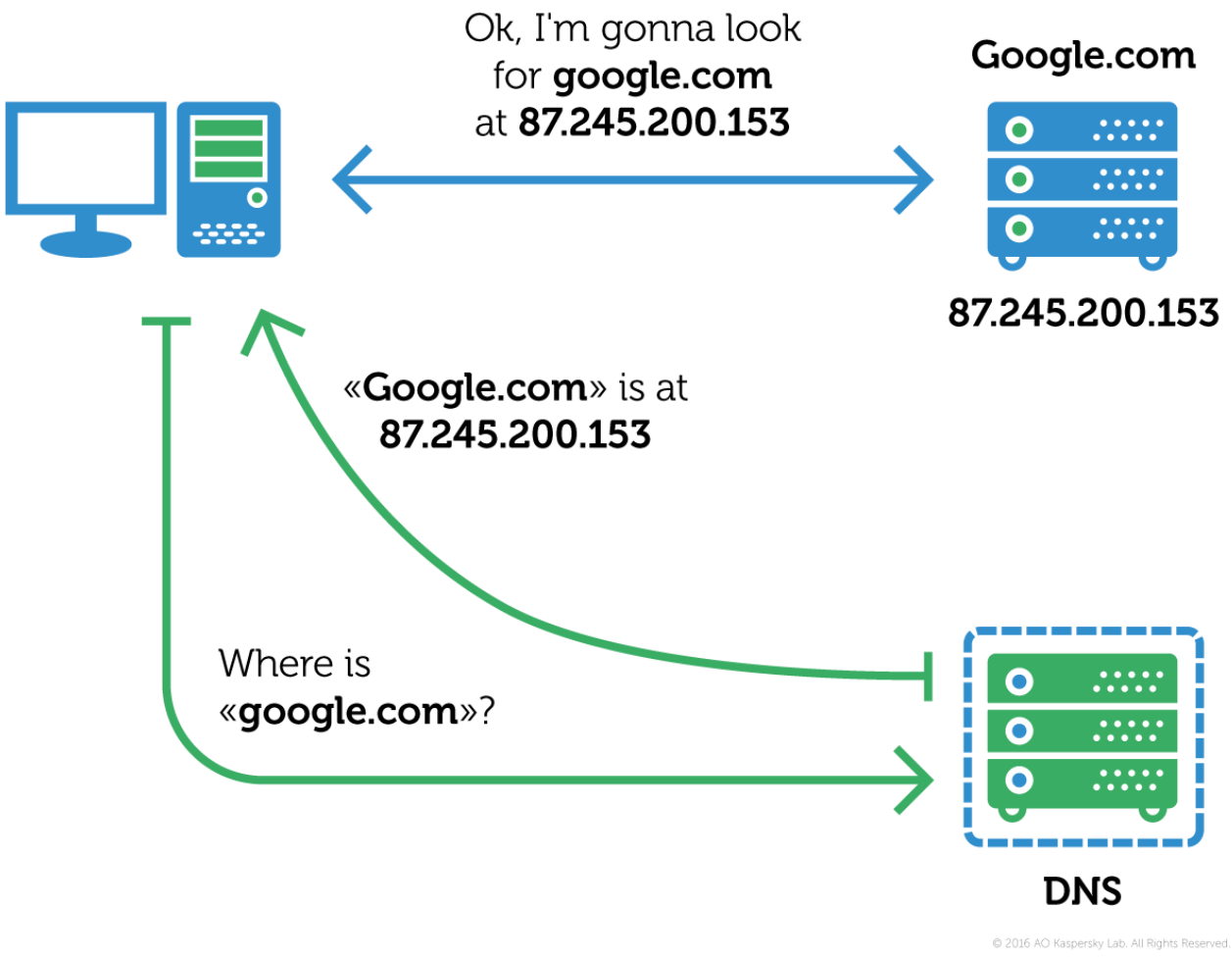
- Resources
  - http://radioopensource.org/the-five-nsa-programs-you-should-know-about/
  - https://www.cloudwards.net/prism-snowden-and-government-surveillance/
  - https://www.propublica.org/article/nsa-data-collection-faq
  - https://en.wikipedia.org/wiki/XKeyscore
  - wikiwand.com/en/MUSCULAR_(surveillance_program)
  - https://www.wikiwand.com/en/List_of_government_mass_surveillance_projects


ow the NSA collects your data
Content
Metadata
Info Sharing
RCES
Telecommunications Cables
AT&T
VERIZON
SPRINT
FACEBOOK
APPLE
GOOGLE
MICROSOFT
YAHOO
AOL
PATRIOT ACT
Section 215
FISA AMENDMENT
Section 702
GCHQ
FAIRVIEW, STORMBREW, BLARNEY, AND OAKSTAR
("Upstream" Data)
PRISM
(Internet Content)
MAINWAY
Phone Metadata)
NUCLEON
(Phone Content)

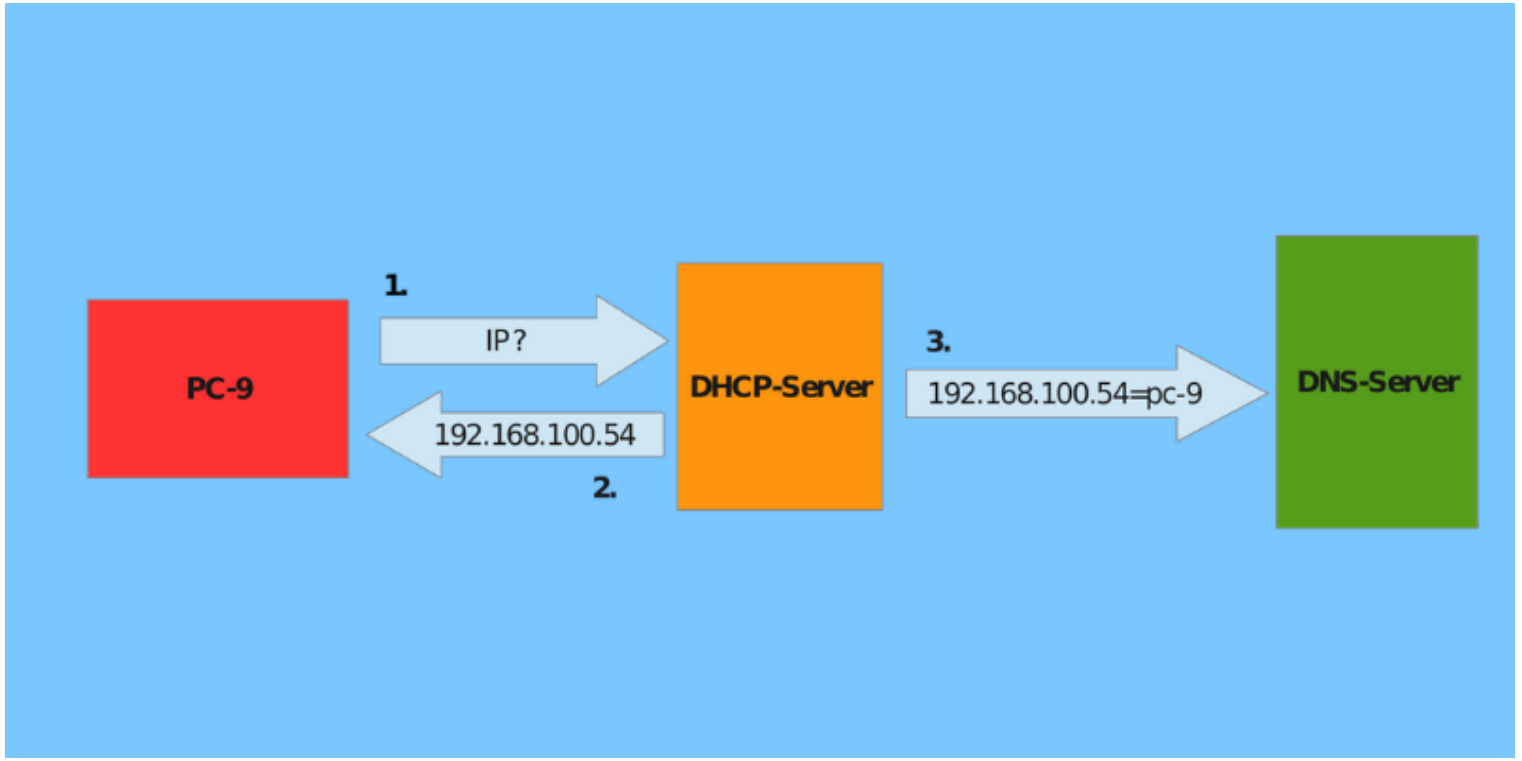
PRISIM

Before we go further… What is the Internet?

DNS



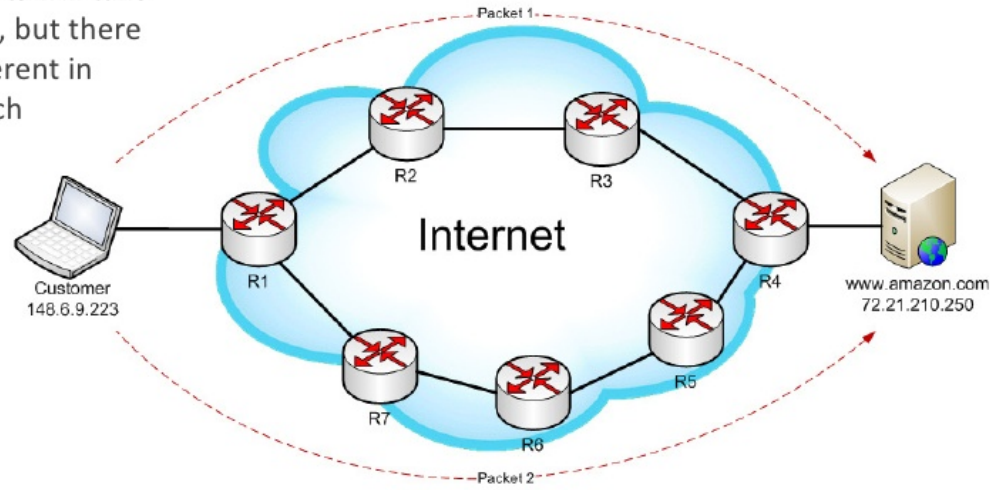
DHCP


PC-9
1.
IP?
192.168.100.54
2.
DHCP-Server
3.
192.168.100.54=pc-9
DNS-Server

Static packet routing

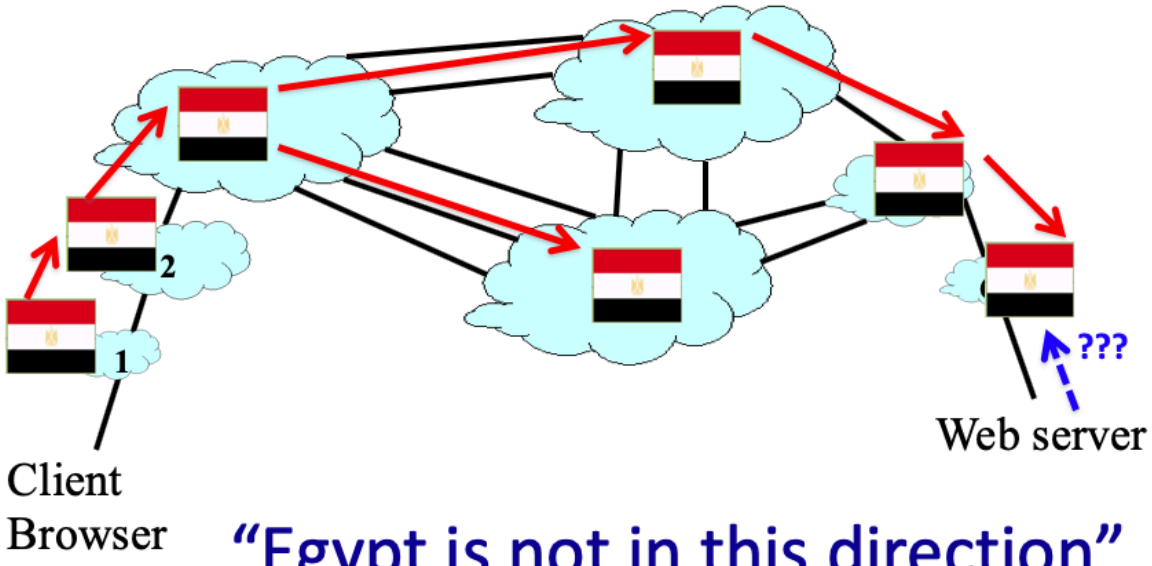
Packet Switching Overview

- In **packet-switching**, the packets are sent towards the destination irrespective of each other
- There is no predetermined path; each router makes a **local** decision as to how to forward the packet towards it intended destination
- Typically packets will take the same path, but there is nothing inherent in IP routing which dictates that each packet must take the same path



ShortestPathFirst Consulting Services
www.shortestpathfirst.net

Withdrawing a traffic route



"Egypt is not in this direction"

Internet Traffic to/from Egypt (2011)

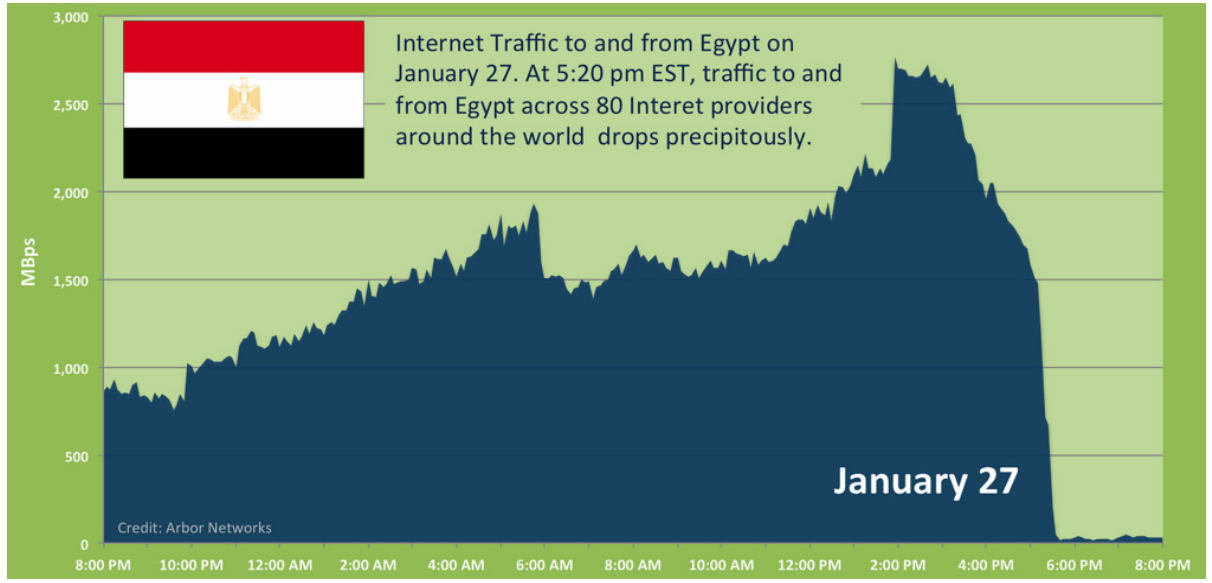
Egypt blocks Internet access amid protests

28 JANUARY 2011 **Daniel Shane**

Government orders telcos to block web access as protestors take to the streets

The Egyptian government has called on telecommunications providers in the country to block access to the Internet in response to widespread civil unrest.

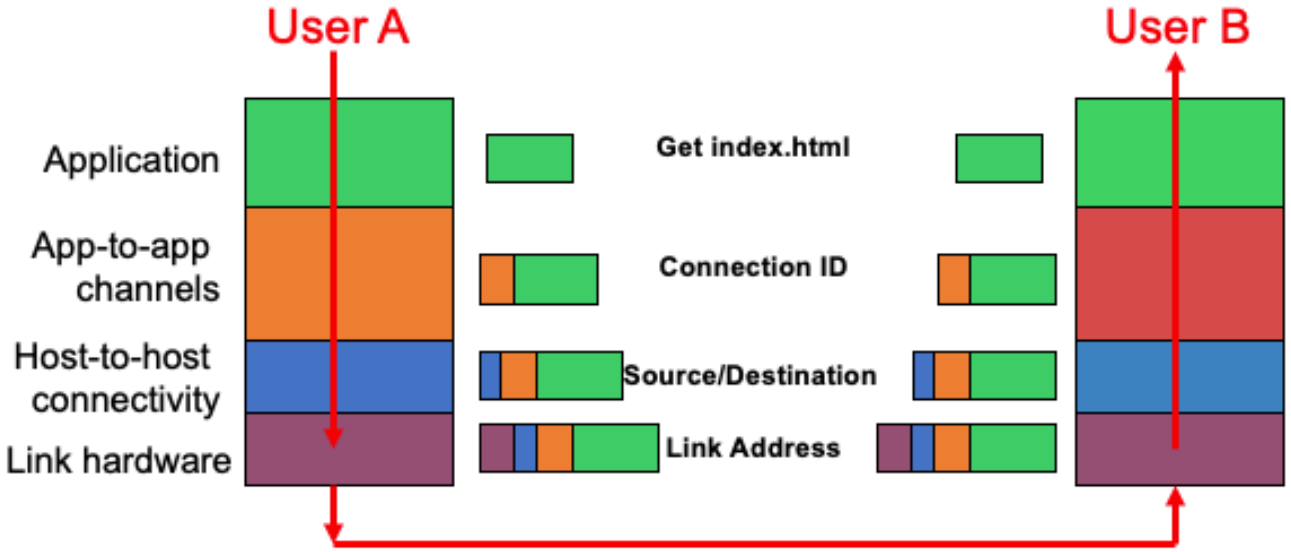
Vodafone Egypt, one of the largest operators in the country not controlled by the state, today said it has disabled access following pressure from authorities.



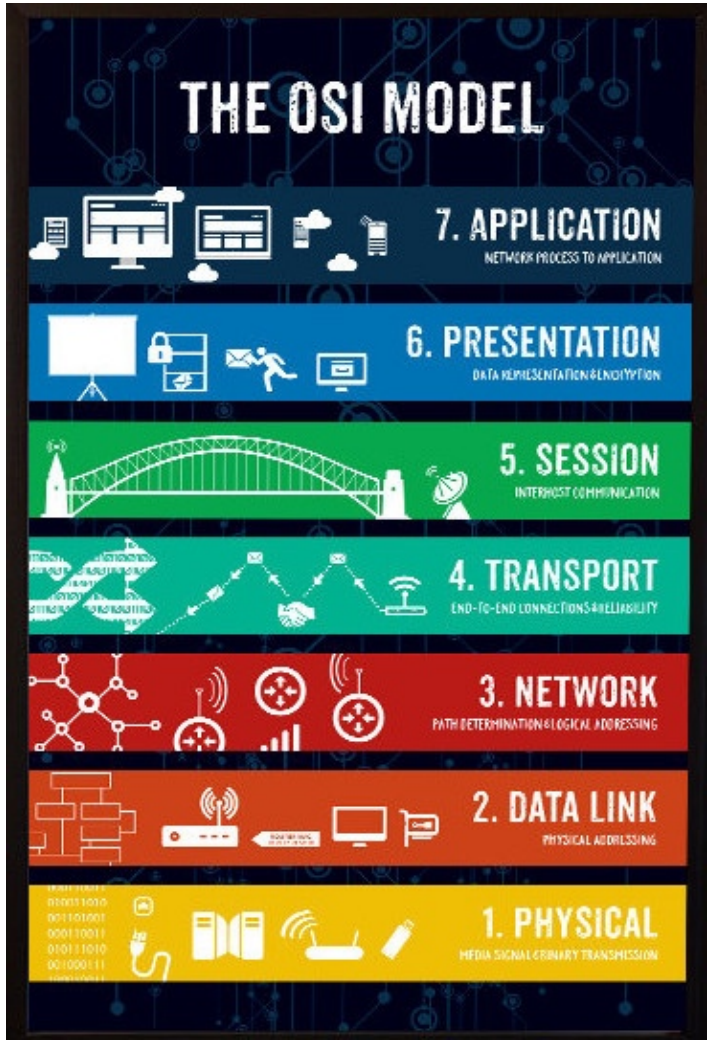
The Internet is like a nesting doll

- Modularity
  - Each layer relies on services from layer below
  - Each layer exports services to layer above
- Interfaces
  - Hides implementation details
  - Layers can change without disturbing other layers

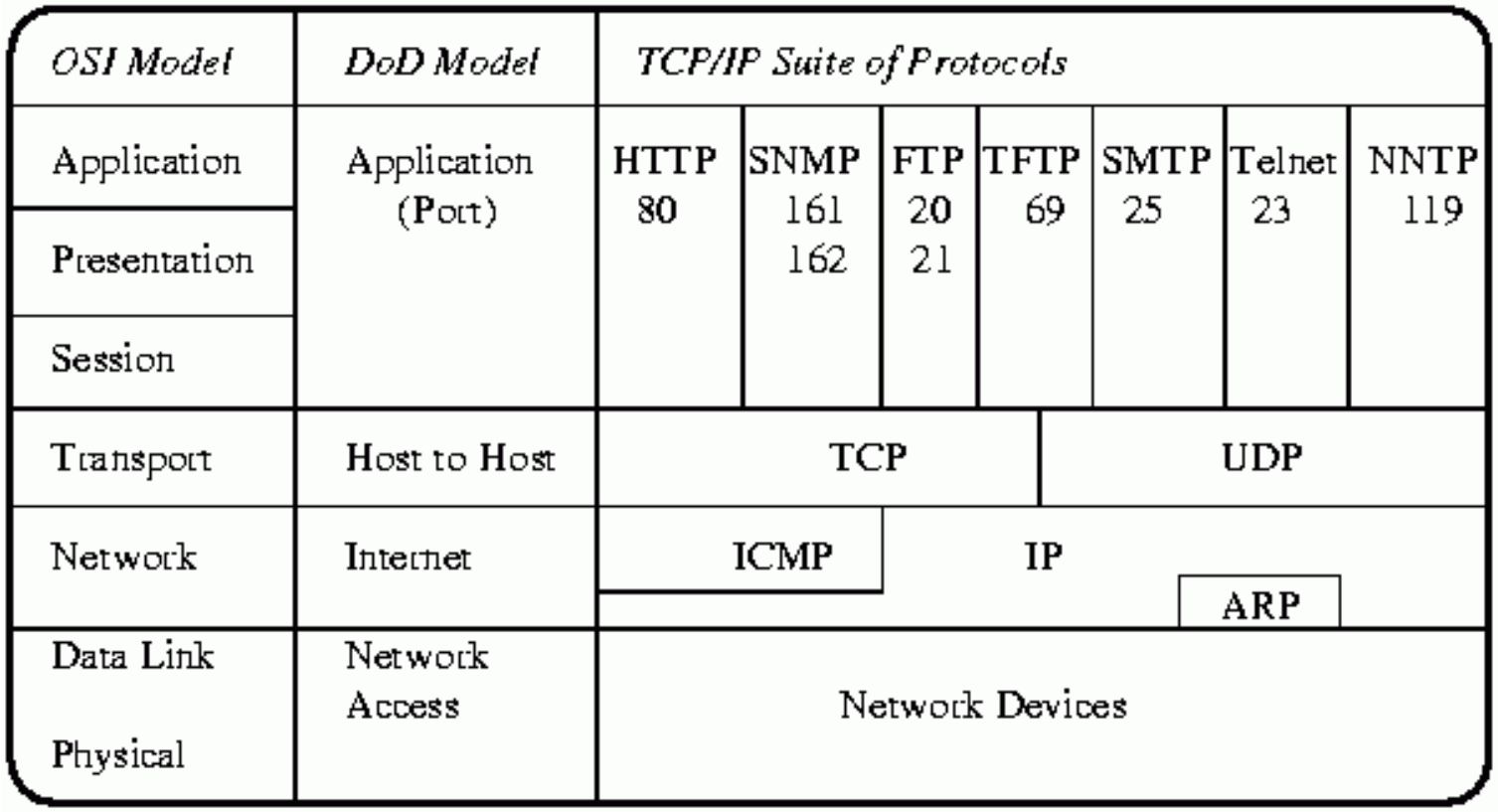
Layer Encapsulation in HTTP



OSI Model


THE OSI MODEL
7. APPLICATION
NETWORK PROCESS TO APPLICATION
6. PRESENTATION
5. SESSION
INTERHOST COMMUNICATION
4. TRANSPORT
END-TO-END CONNECTIONS & RELIABILITY
3. NETWORK
PATH DETERMINATION & LOGICAL ADDRESSING
2. DATA LINK
PHYSICAL ADDRESSING
1. PHYSICAL

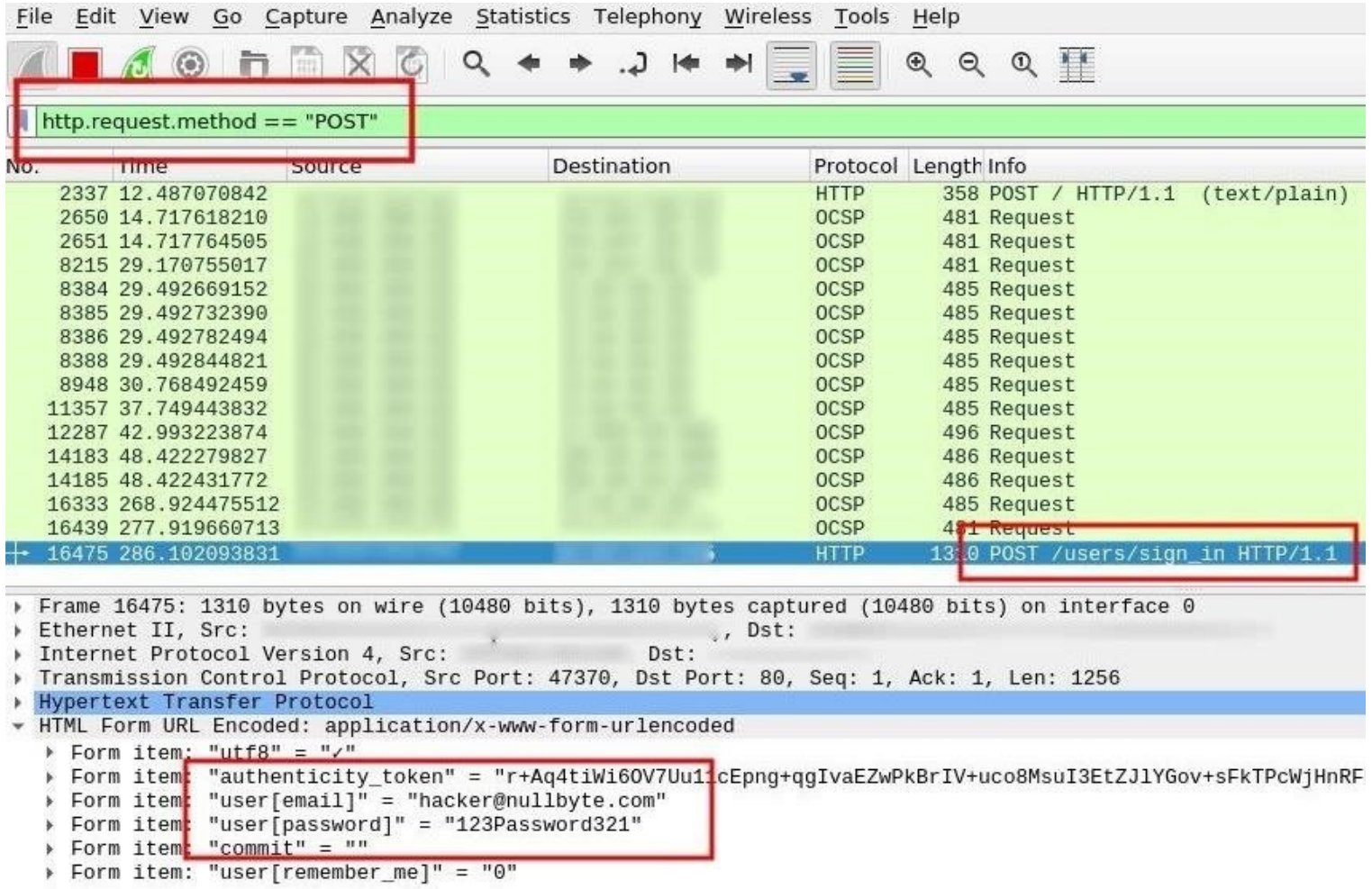
OSI Model


OSI Model
DoD Model
TCP/IP Suite of Protocols
Application
Presentation
Session
Application (Port)
HTTP 80
SNMP 161 162
FTP 20 21
TFTP 69
SMTP 25
Telnet 23
NNTP 119
Transport
Host to Host
TCP
UDP
Network
Internet
ICMP
IP
ARP
Data Link
Physical
Network Access
Network Devices

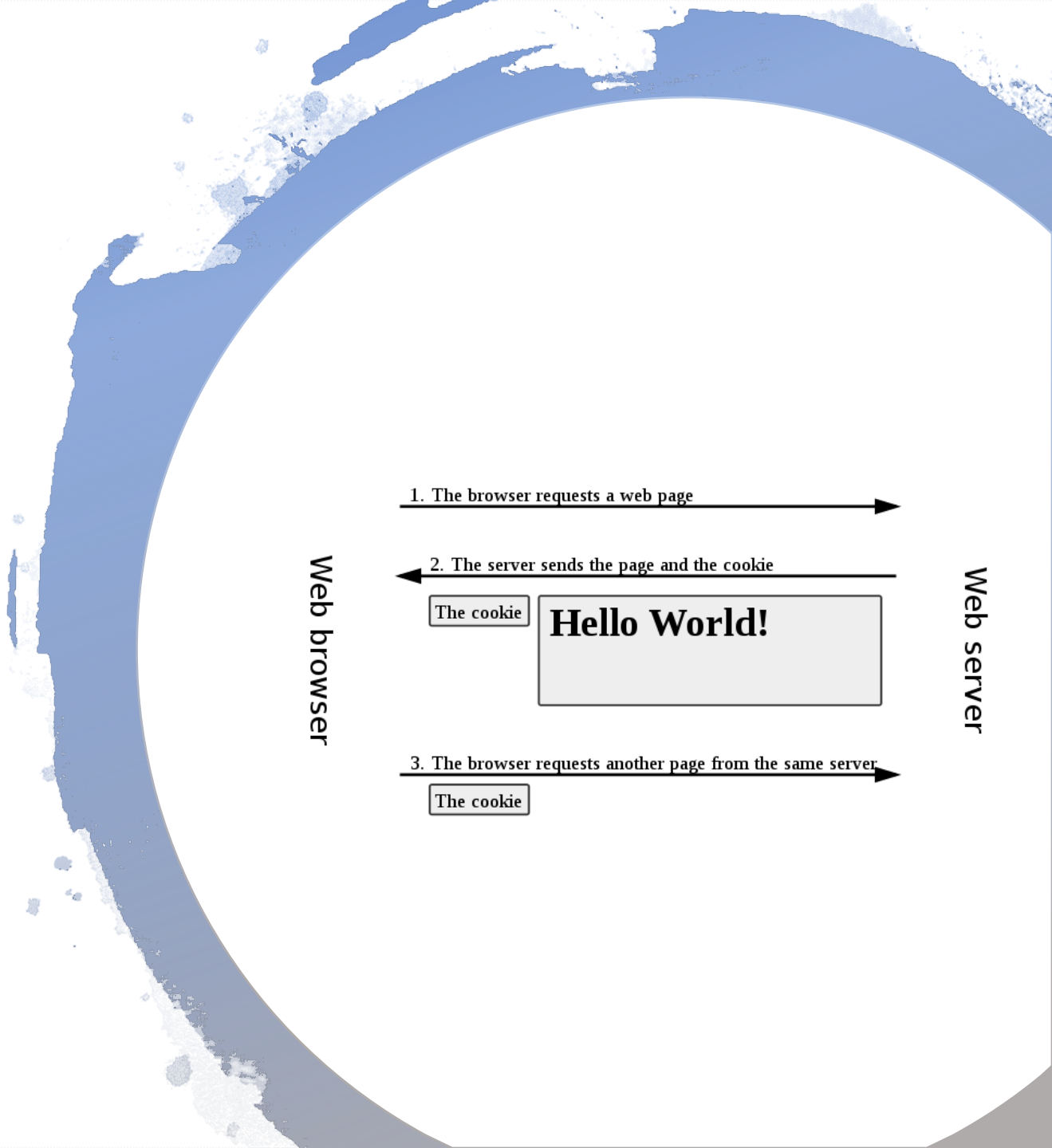
HTTP Response packet

HTTP/1.1 200 OK	**Status Line**	**HTTP Response**
Date: Thu, 20 May 2004 21:12:58 GMT Connection: close	**General Headers**	
Server: Apache/1.3.27 Accept-Ranges: bytes	**Response Headers**	
Content-Type: text/html Content-Length: 170 Last-Modified: Tue, 18 May 2004 10:14:49 GMT	**Entity Headers**	
<html> <head> <title>Welcome to the Amazing Site!</title> </head> <body> This site is under construction. Please come back later. Sorry! </body> </html>	**Message Body**	

The problem without encryption



Supercookies --- What is a regular cookie



Supercookies

- A supercookie is a tracking cookie but has a more sinister use. Supercookies also have different functionality to a regular cookie, too.
- With a regular cookie, if you don't want it to follow you around the internet, you can clear your browsing data, your cookies, and more. You can block cookies and third-party cookies from your browser, and auto-delete cookies after your browser session ends. You have to log into each site again, and your shopping cart items won't store, but it also means tracking cookies are tracking you anymore.
- A supercookie is different. Clearing your browsing data doesn't help. This is because a supercookie isn't really a cookie; it is not stored in your browser.
- Instead, an ISP inserts a piece of information unique to a user's connection into the HTTP header. The information uniquely identifies any device. In the case of Verizon, it allowed the tracking of every website visited.
- Because the ISP injects the supercookie between the device and the server it is connecting too, there's nothing the user can do about it. You cannot delete it, because it isn't stored on your device. Ad and script blocking software cannot stop it, because it happens after the request leaves the device.

Does Internet design prevent misuse?

- Individual endpoints can only use addresses given to them when connect to the network
- Individual end-points can “spoof” any IP address

Does Internet design prevent misuse?

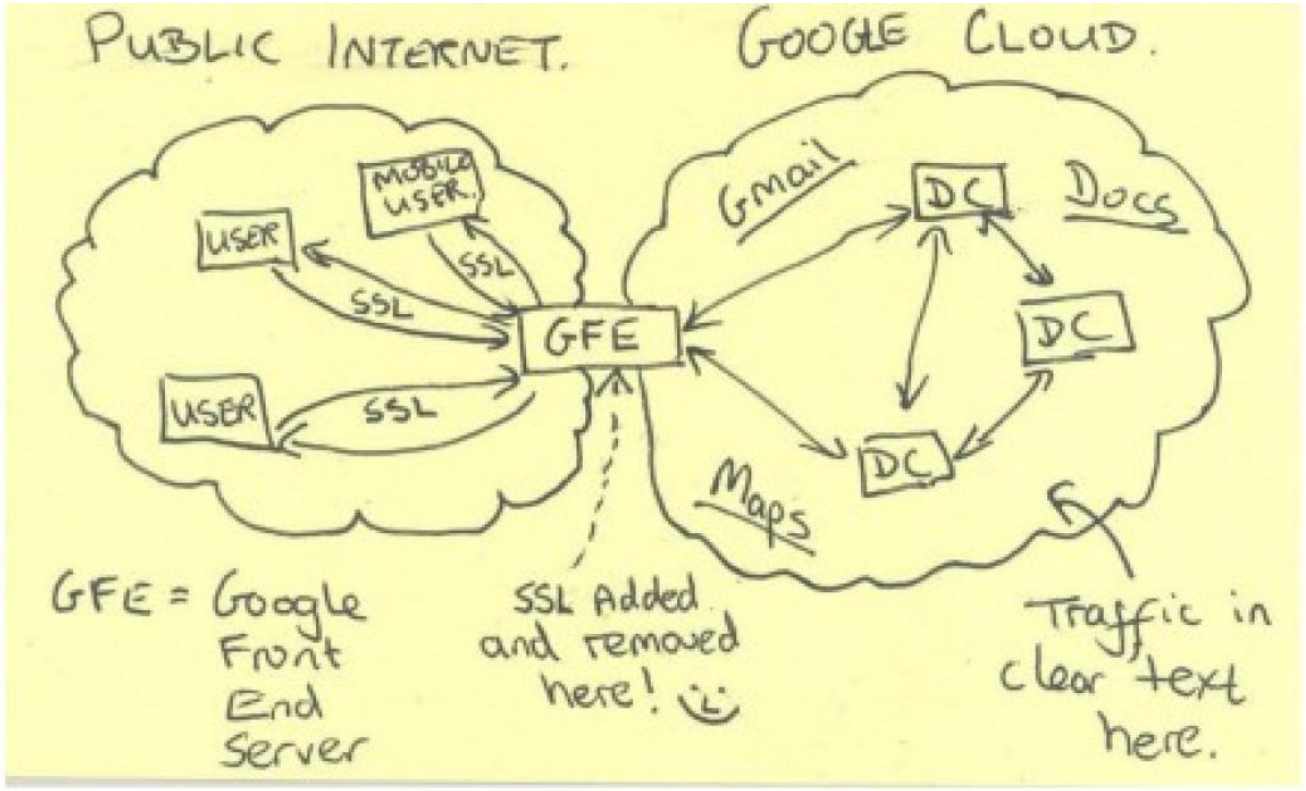
Networks are assigned unique IP address blocks from a central authority ("IANA"): Princeton has 128.112.*

A. Network can only announce assigned addresses

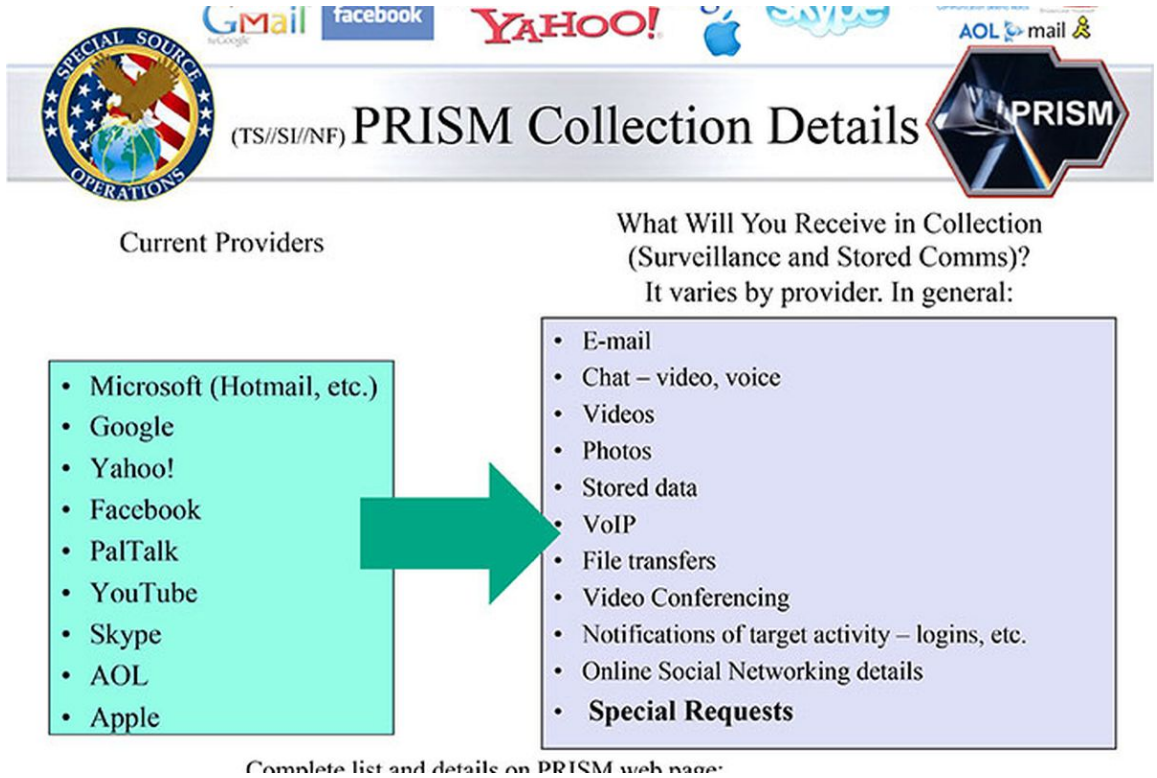
B. Networks can spoof any address

That brings us back to PRISM

The drawing



TOP SECRET//SI//NOFORN


(TS//SI//NF) PRISM Collection Details
PRISM
Current Providers
What Will You Receive in Collection (Surveillance and Stored Comms)? It varies by provider. In general:
Microsoft (Hotmail, etc.)
Google
Yahoo!
Facebook
PalTalk
YouTube
Skype
AOL
Apple
E-mail
Chat – video, voice
Videos
Photos
Stored data
VoIP
File transfers
Video Conferencing
Notifications of target activity – logins, etc.
Online Social Networking details
Special Requests
Complete list and details on PRISM web page:

1
PUBLIC INTERNET

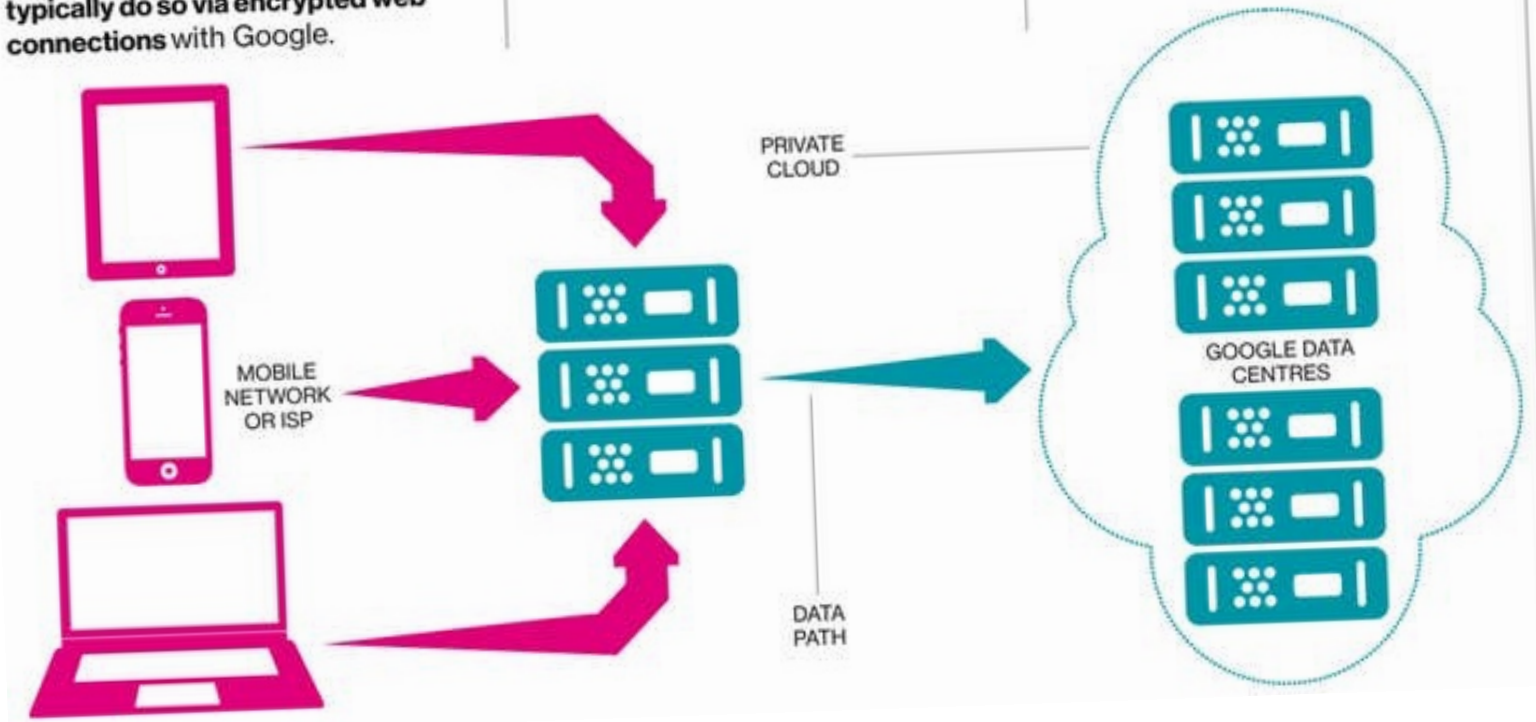
Internet and mobile users who send Gmail, create Google Drive documents or use other Google services over **public internet typically do so via encrypted web connections** with Google.

2
FRONT-END SERVERS

All Google requests are received by front-end servers that handle and process web requests, returning data to the user.

3
GOOGLE'S PRIVATE CLOUD

Google's data centres, located around the world, **are networks of computers linked by private fibre-optic cables.**



4
GOOGLE'S GLOBAL INFRASTRUCTURE

Cloud companies store multiple copies of user data in geographically distributed data centres to improve reliability and performance.

They generally connect their data centres over privately owned or leased fibre-optic cables, which do not share traffic with other internet users. Until recently, these internal data networks were not encrypted.

Google announced in September, however, that it is moving quickly to encrypt those connections.

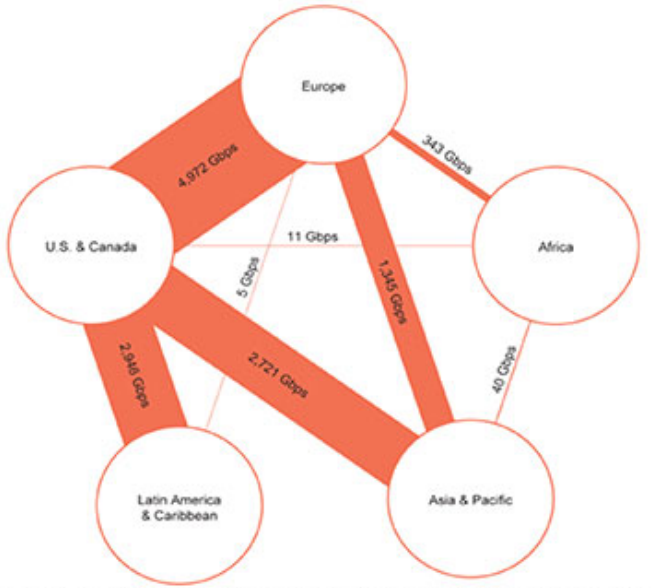
SOURCE:WASHINGTON POST

TOP SECRET//SI//ORCON//NOFORN

(TS//SI//NF) Introduction

U.S. as World's Telecommunications Backbone

- Much of the world's communications flow through the U.S.
- A target's phone call, e-mail or chat will take the **cheapest** path, **not the physically most direct** path – you can't always predict the path.
- Your target's communications could easily be flowing into and through the U.S.



International Internet Regional Bandwidth Capacity in 2011

Source: Telegeography Research

TOP SECRET//SI//ORCON//NOFORN

What does the future hold?

Curation of content

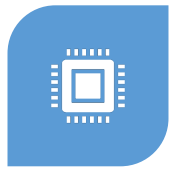
Is this the worst things have ever been?

Why surveillance may not be a bad thing….

HACK THE VOTE

TIME OF PEACE

MALWARE



EASE OF HACKING

MEDICAL DEVICES

THERMOSTATS

CAR HACKING

The hacks you don’t hear about…

US Electricity Grid – 2017

FBI Report - “a multi-stage intrusion campaign by cyber actors who…..conducted spear phishing, and gained remote access into energy sector networks. After obtaining access, they conducted network reconnaissance, moved laterally, and collected information pertaining to Industrial Control Systems.”

Federal Aviation Administration – 2015

Although the 2015 event targeted administrative systems and was quickly contained, it raised the specter of hackers shutting down radar or sending false information to aircraft systems — concerns that were echoed in a report following the incident.

SWIFT – 2015

Trust and integrity are central to SWIFT’s business model, but in 2015 those values were overturned with a series of real-life cyber-attacks that resulted in sizable losses. The main attack centered on the Bangladesh Central Bank (BCB), with criminals attempting an eye-watering theft of $1 billion. United States

Central Command (CENTCOM) – 2008

Back in 2008, US Central Command (CENTCOM) was the military center for the United States military’s Middle East operations. A USB drive, found in a parking lot and containing the agent.btz worm, was inserted into a laptop connected to the CENTCOM network. From there it spread undetected to other systems, both classified and unclassified.

US Healthcare Network – 2016

SamSam ransomware attacks took place over three years, extorting $6 million in payments and resulting in $30 million in damages.

Stuxnet

Bibliography

- I’m not being graded so…
  - **The Internet**

Questions?