It’s a brave new world !

Opportunities, risks and security threats in an EU digitized society

Juan Antonio Cordero Fuertes, *École polytechnique*

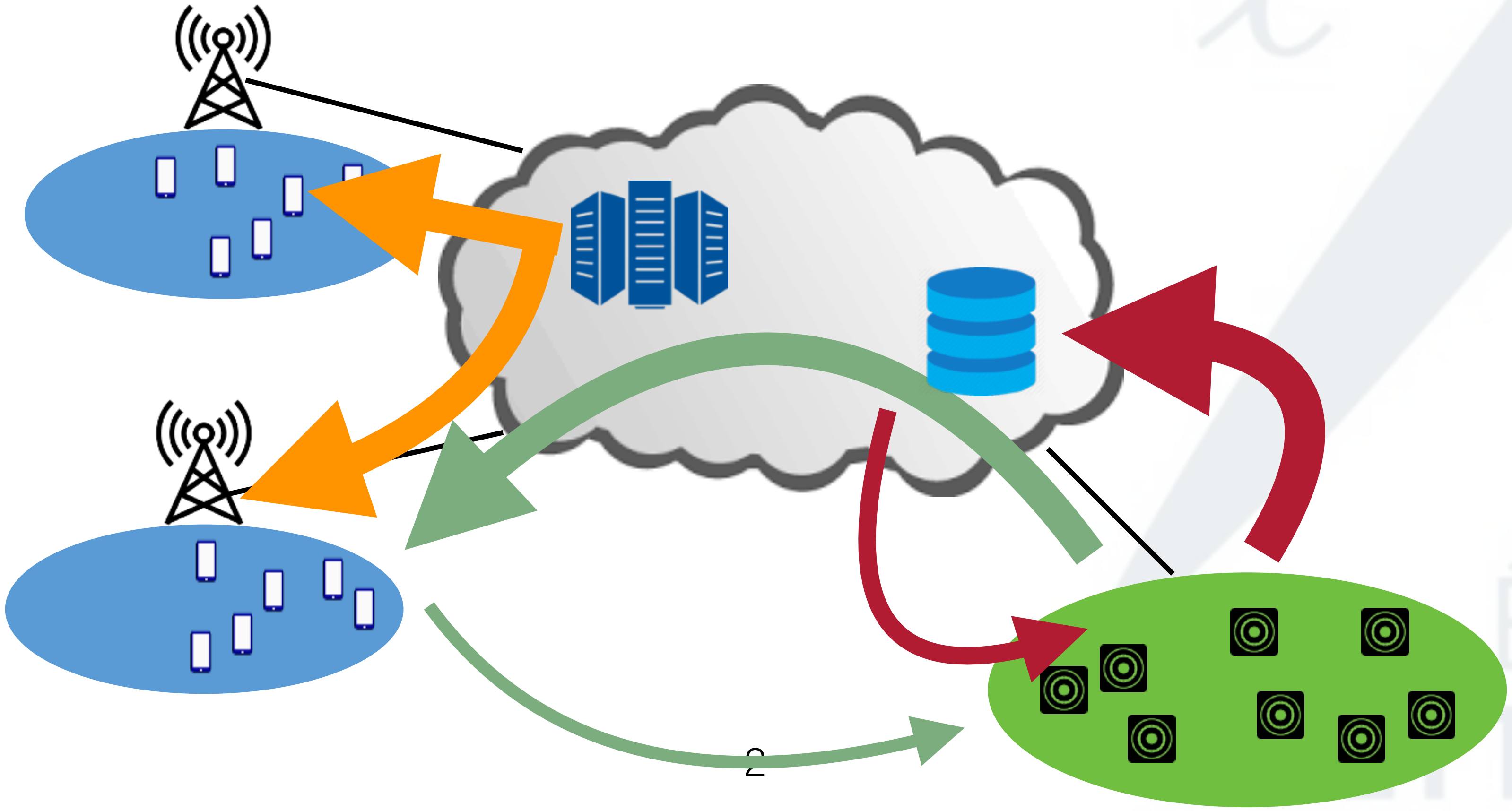
European Documentation Center, Universidad Autónoma de Barcelona
December 2018

Towards a digitized society

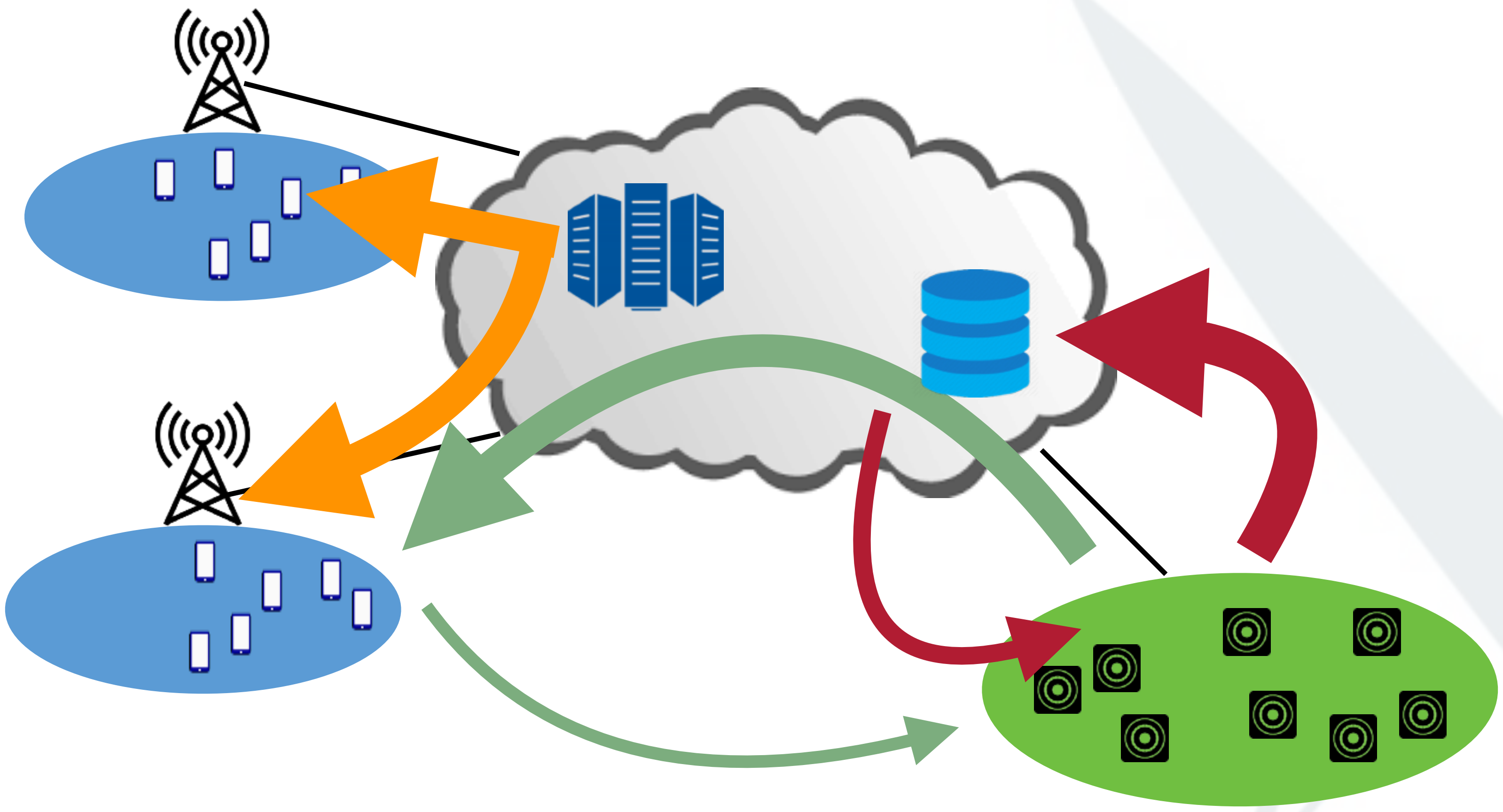
- **Digitization** : mobiles and “things”, with pre-existing infrastructures relying on the Internet

- Mobiles : smartphone traffic to exceed PC traffic — mostly for video consumption

- “Things”: cheap, low-powered, connectable sensoring devices with unique ids
  - Systems based on “things” to collect, aggregate and process huge amounts of data (IoT)
  - “Sensors” collecting data, connected to “machines” processing it
  - ~50 billion “things” to be connected in 2020 (Evans, 2011)
  - Use cases : Smart Grid, smart cities, agricultural sensor networks, connected healthcare



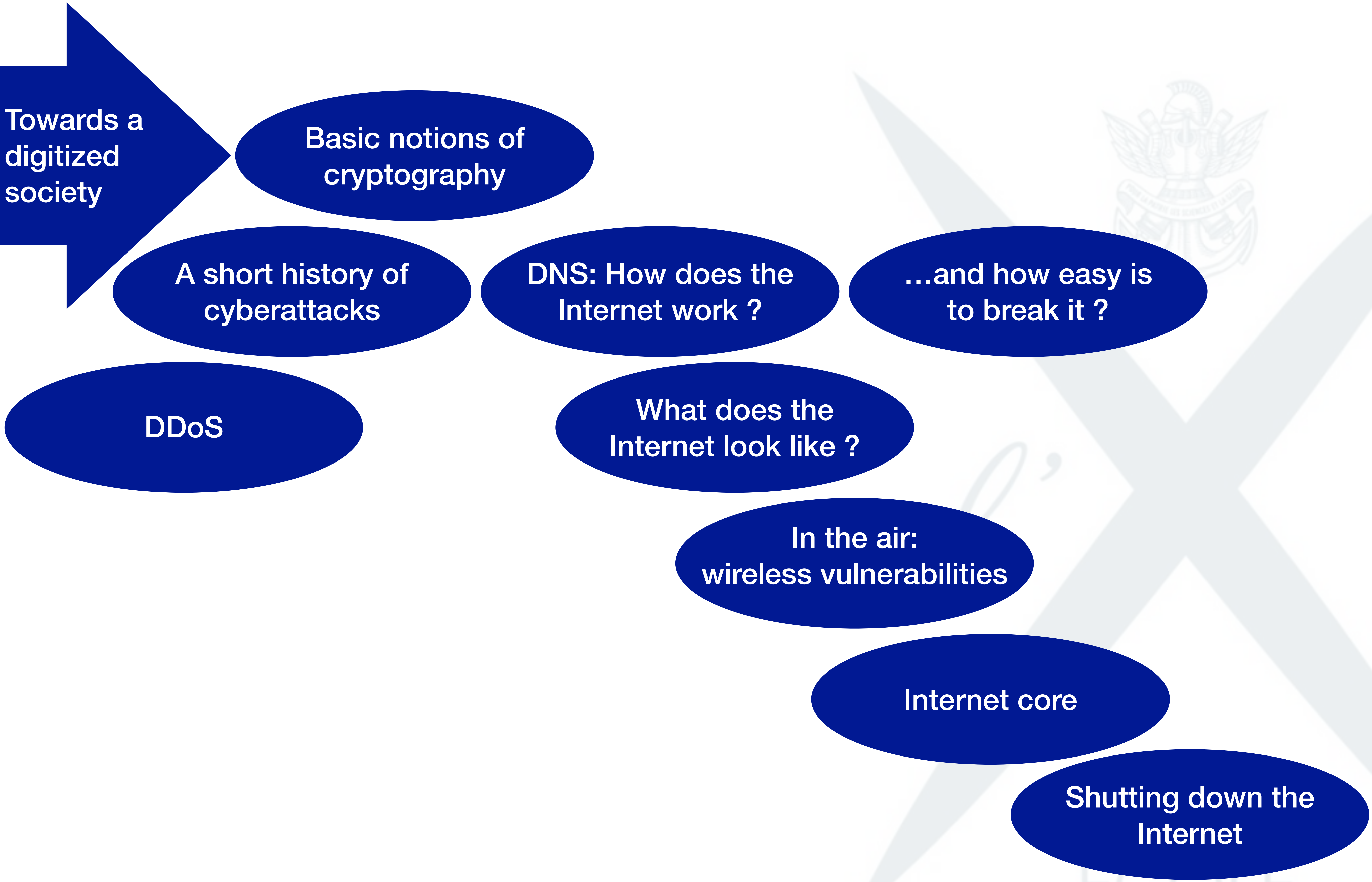
Towards a digitized society



“*The Internet beyond the Internet*”

⬇

Which implications for cybersecurity ?



Towards a digitized society

Basic notions of cryptography

A short history of cyberattacks

DNS: How does the Internet work ?

...and how easy is to break it ?

DDoS

What does the Internet look like ?

In the air: wireless vulnerabilities

Internet core

Shutting down the Internet

Basic cryptography

- What typically matters in communication ?
  - Data confidentiality
  - Data integrity
  - Entity authentication

- Classic risks
  - Passive eavesdropping
  - Data forging
  - Identity spoofing

Basic cryptography for a digitized society

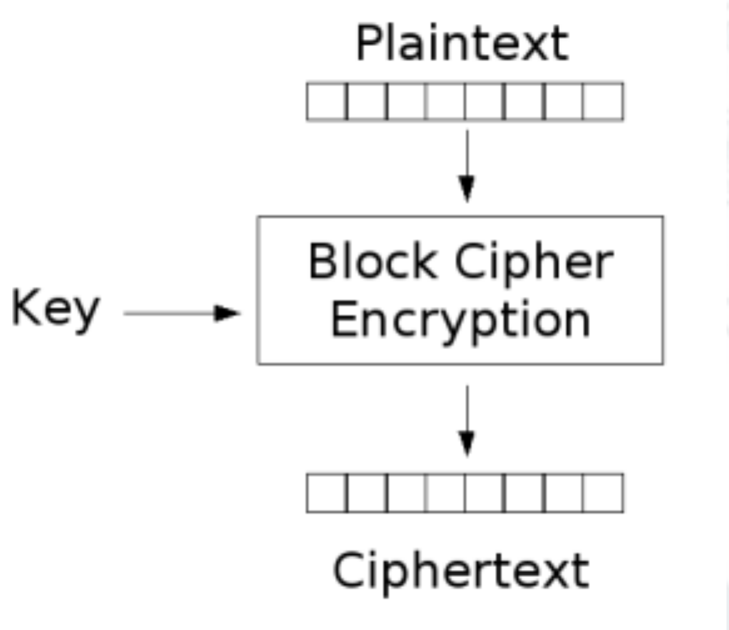
- What typically matters in communication ?
  - Data confidentiality
  - Data integrity
  - Entity authentication

- Classic risks
  - Passive eavesdropping
  - Data forging
  - Identity spoofing

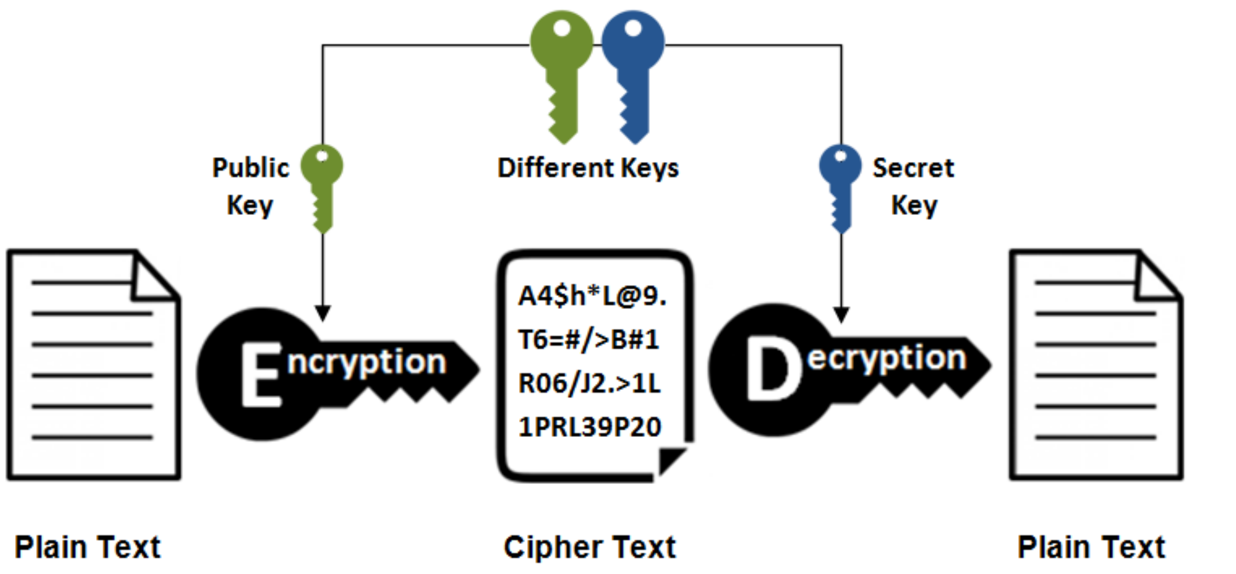
- Risks in **connected infrastructures and services**
  - Network intrusion
  - Data exfiltration, manipulation, ransomware attacks
  - Denial of Service (DoS) and Distributed DoS (DDoS) attacks
  - Phishing, service malfunction, Man in the Middle (MitM)

Basic cryptography

- **Symmetric encryption** : one key to rule ’em all
  - e.g. AES (Advanced Encryption Standard)
  - Strength depends on the *key length*



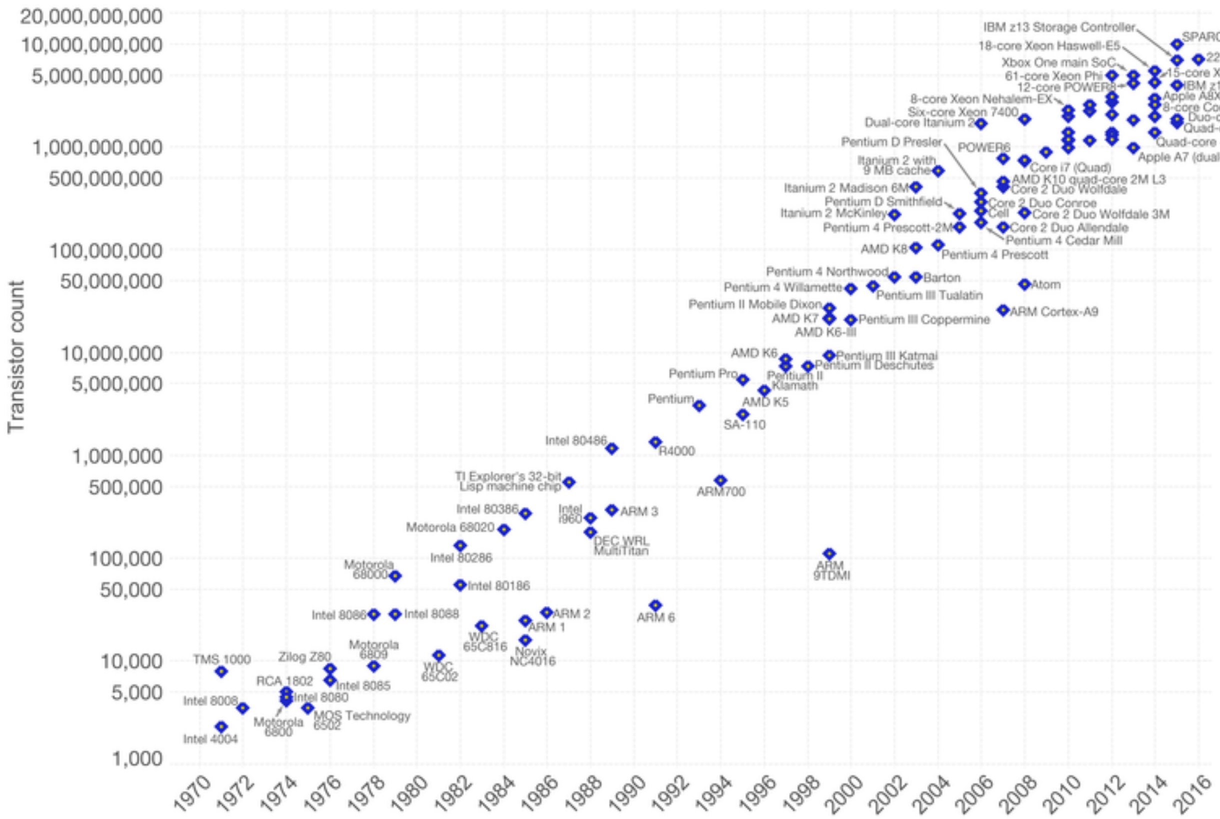
- Public and private keys : **asymmetric encryption**
  - e.g. RSA, El-Gamal
  - Strength depends on the *practical impossibility to reverse a mathematical operation*
    - one-way functions, P≠NP
  - Ex: factorization, discrete logarithm



(ref: https://medium.com/@User3141592/notes-on-computational-cryptography-98db5f2908f1)

Moore’s Law

Number of transistors on integrated chips (1971-2016)



Data source: Wikipedia (https://en.wikipedia.org/wiki/Transistor_count)
The data visualization is available at OurWorldinData.org. There you find more visualizations and research on this topic.

Licensed under CC-BY-SA by the author Max Roser.

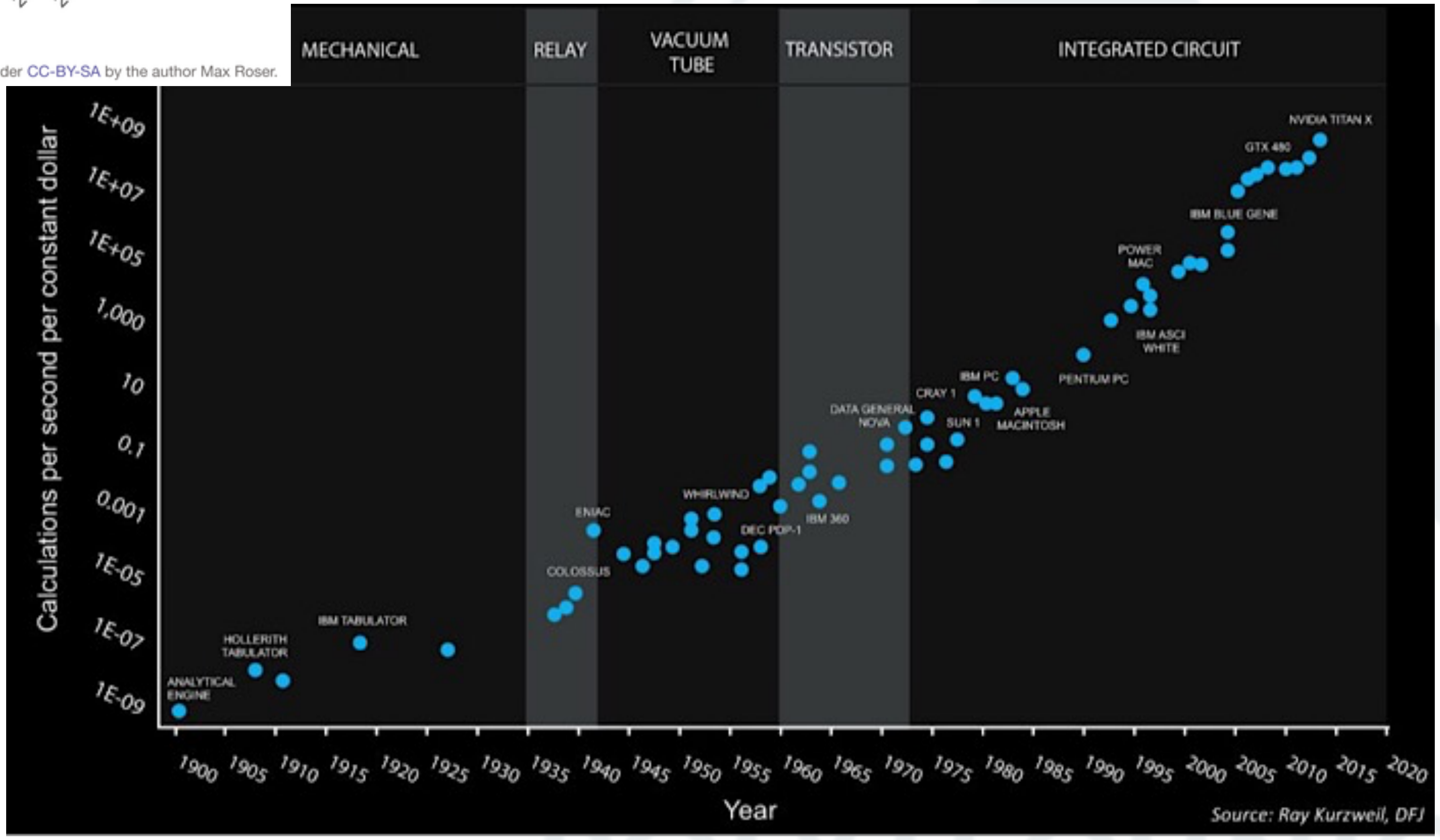
Slightly different flavours, but same message:

“computing capacity (or # transistors per IC) ***duplicates*** *roughly* ***every 2 years****”*

- Other ex.: price of electronic products, processing speed of μprocessors
- Empirical observation

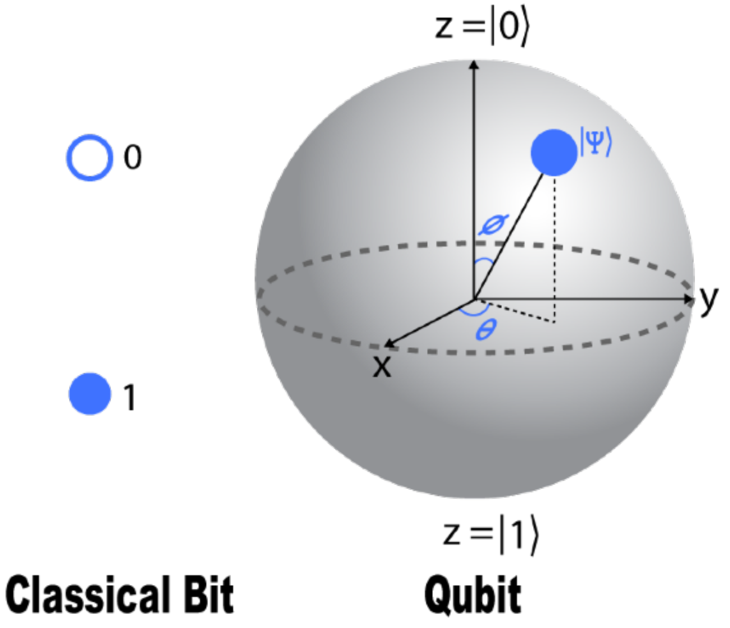
If computing capacity increases, *keys need to be longer to remain effective*

(otherwise it’s easy to try all possible combinations)



Source: Ray Kurzweil, DFJ

Quantum computing



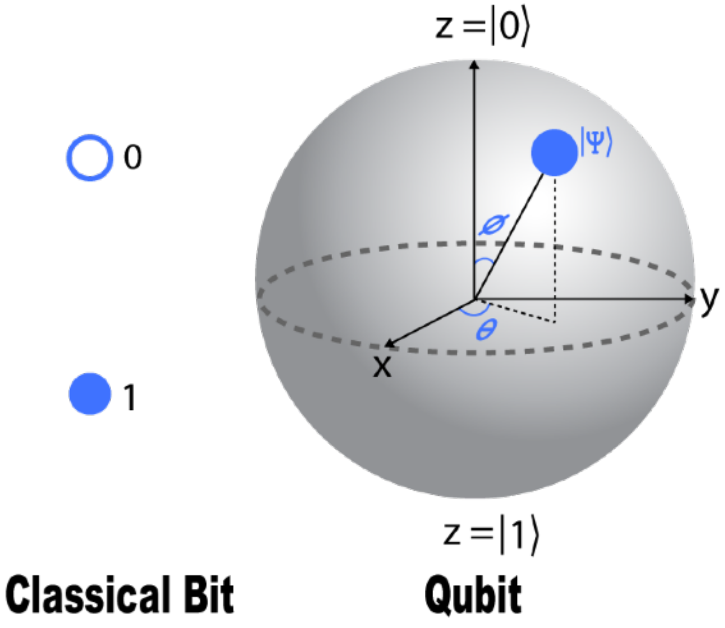
- Physical quantum phenomena
  - Superposition
  - Entanglement

"Information stored in a set of qubits scales ***exponentially****"* **

(2^N-1 bits for N qubits)

** With many caveats.

Quantum computing



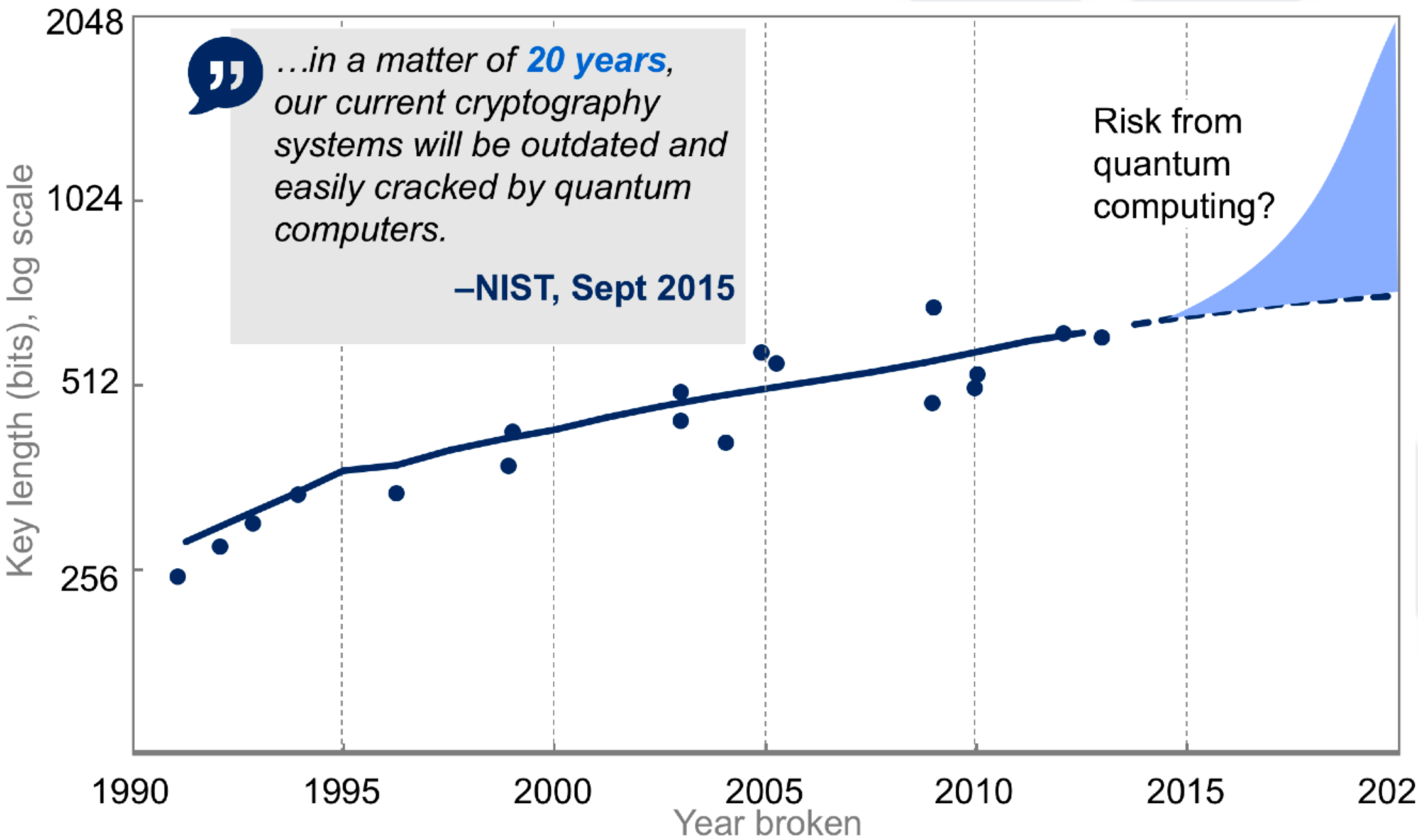
- Physical quantum phenomena
    - Superposition
    - Entanglement

“Information stored in a set of qubits scales ***exponentially****”* **

(2^N-1 bits for N qubits)

Shor’s quantum algorithm (1994) solves integer *factorization* in *polynomial* (not exponential) time

- If implemented, RSA (and, all mechanisms relying on the “difficulty” of factorization) would be compromised
- Even very long keys for today’s standards (e.g. 2048) may become insecure



*…in a matter of **20 years**, our current cryptography systems will be outdated and easily cracked by quantum computers.*

–NIST, Sept 2015

Risk from quantum computing?

Breaks of the RSA cryptosystem using conventional computation

** With many caveats.

Cryptography and cybersecurity

- Cryptographic primitives are in the **core** or all security mechanisms in the Internet *(…not only for encryption purposes !)*
  - Digital signatures and certificates
  - Hashes
  - Key distribution and management schemes

- But, cybersecurity is **not** only about cryptography*
  - Broader domain: “technologies, processes and controls designed to protect systems, networks and data from cyber attacks”
  - Three pillars: people, processes, technology (crypto included)
  - *…weakest link is typically **not** the cryptographic part*

* Crypto is actually a small part of cybersec.

Cryptography and cybersecurity

- Cryptographic primitives are in the **core** or all security mechanisms in the Internet *(…not only for encryption purposes !)*
  - Digital signatures and certificates
  - Hashes
  - Key distribution and management schemes

- But, cybersecurity is **not** only about cryptography*
  - Broader domain: “technologies, processes and controls designed to protect systems, networks and data from cyber attacks”
  - Three pillars: people, processes, technology (crypto included)
  - *…weakest link is typically **not** the cryptographic part*

* Crypto is actually a small part of cybersec.

Some (more or less famous) relevant cyberattacks

1988 : Morris worm

First DDoS attack, ~6000 computers affected (10% Internet devices at the time), ~100M USD damage

1999 : Melissa

Virus spread as mail attachment, using MS-Office to propagate, 80M USD damage

1999 : NASA & DoD hacks

By teenager Jonathan James, 40K USD damage

2000 : Mafiaboy

DDoS attack against Amazon, eBay, Yahoo!, ~1200M USD damage

2002 : DNS root attacks

1 hour DDoS attack against the 13 root servers of DNS

2013 : Yahoo!

Attacks on Yahoo!, 500M and 1000M accounts compromised

2014 : Google DNS 8.8.8.8

BGP attack against 8.8.8.8: traffic re-routed towards Venezuela, Brazil

2015, 16 : AshleyMadison, AdultFriendFinder attacks

60 GB of account information and 400M accounts compromised, respectively. Poor password protection (SHA-1).

2016 : DynDNS attack

DDoS attack affecting Dyn's clients such as GitHub, Twitter, Spotify, Paypal, etc. Hacked IOT devices (~50K in 164 countries), infected by Mirai malware, used as "zombie armies". Traffic peaks of 280 Gbps

2018 : WannaCry

Ransonware attack (NHS, Telefonica, FedEx, etc.) exploiting MS SMB protocol vulnerability in Windows, 100 countries affected, 4000M USD damage estimated

Sources: https://www.gomindsight.com/blog/history-of-cyber-attacks-2018/, https://www.arnnet.com.au/slideshow/341113/top-10-most-notorious-cyber-attacks-history/, https://thehackernews.com/2014/03/google-public-dns-server-traffic.html

Some (more or less famous) relevant cyberattacks

1988 : Morris worm

First DDoS attack, ~6000 computers affected (10% Internet devices at the time), ~100M USD damage

1999 : Melissa

Virus spread as mail attachment, using MS-Office to propagate, 80M USD damage

1999 : NASA & DoD hacks

By teenager Jonathan James, 40K USD damage

2000 : Mafiaboy

DDoS attack against Amazon, eBay, Yahoo!, ~1200M USD damage

2002 : DNS root attacks

1 hour DDoS attack against the 13 root servers of DNS

2013 : Yahoo!

Attacks on Yahoo!, 500M and 1000M accounts compromised

2014 : Google DNS 8.8.8.8

BGP attack against 8.8.8.8: traffic re-routed towards Venezuela, Brazil

2015, 16 : AshleyMadison, AdultFriendFinder attacks

60 GB of account information and 400M accounts compromised, respectively. Poor password protection (SHA-1).

2016 : DynDNS attack

DDoS attack affecting Dyn's clients such as GitHub, Twitter, Spotify, Paypal, etc. Hacked IOT devices (~50K in 164 countries), infected by Mirai malware, used as "zombie armies". Traffic peaks of 280 Gbps

2018 : WannaCry

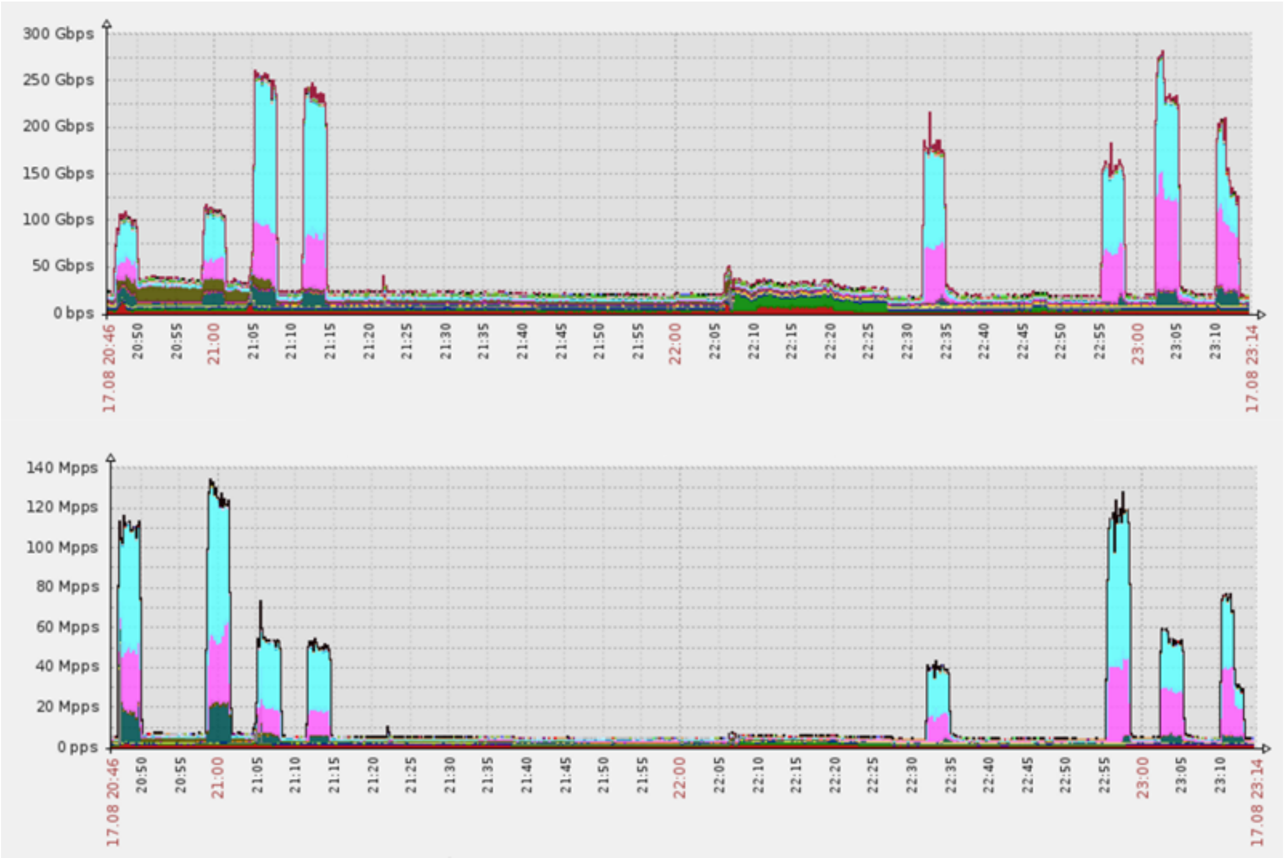
Ransomware attack (NHS, Telefonica, FedEx, etc.) exploiting MS SMB protocol vulnerability in Windows, 100 countries affected, 4000M USD damage estimated

Distributed Denial of Service (DDoS)

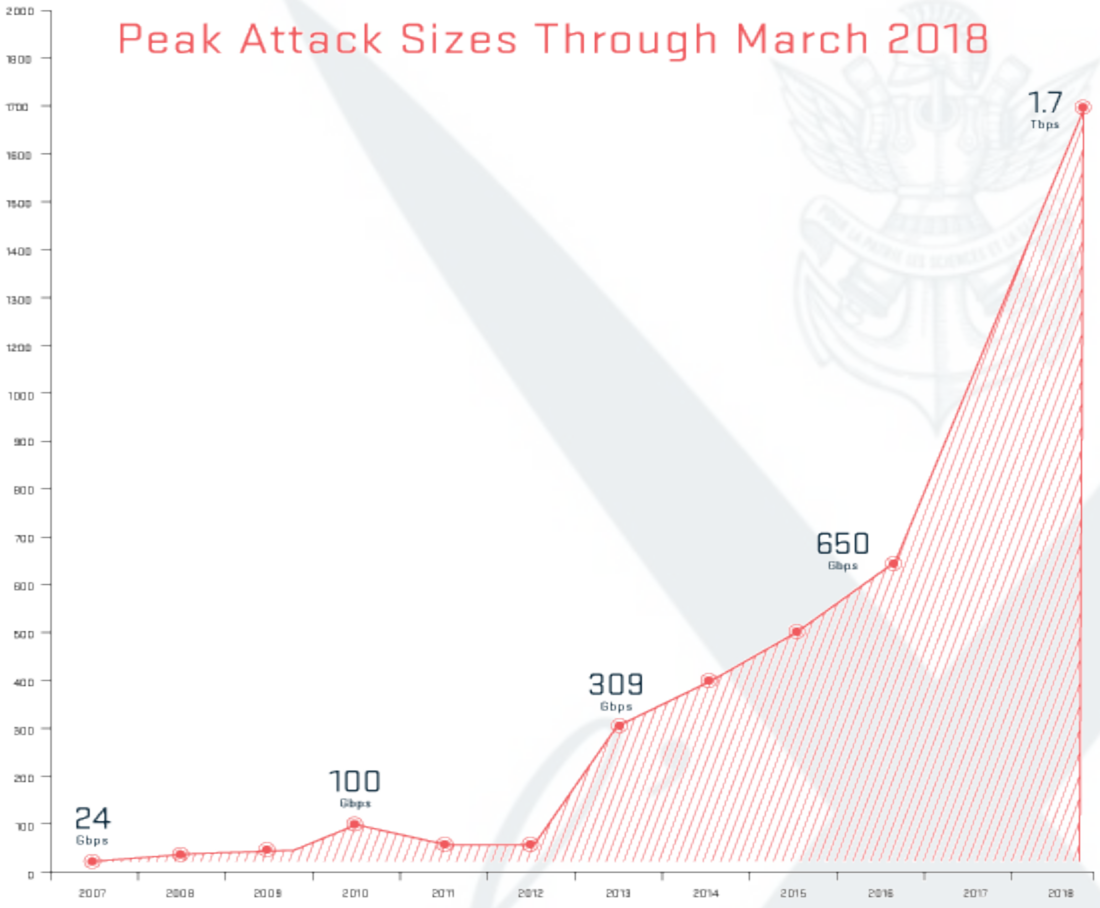
A DDoS is a malicious attempt, by **multiple compromised (and coordinated) systems**, to disrupt normal traffic of a targeted **server**, **service** or **network** by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic.

t.com/blog/history-of-cyber-attacks-2018/,
how/341113/top-10-most-notorious-cyber-
rnews.com/2014/03/google-public-dns-

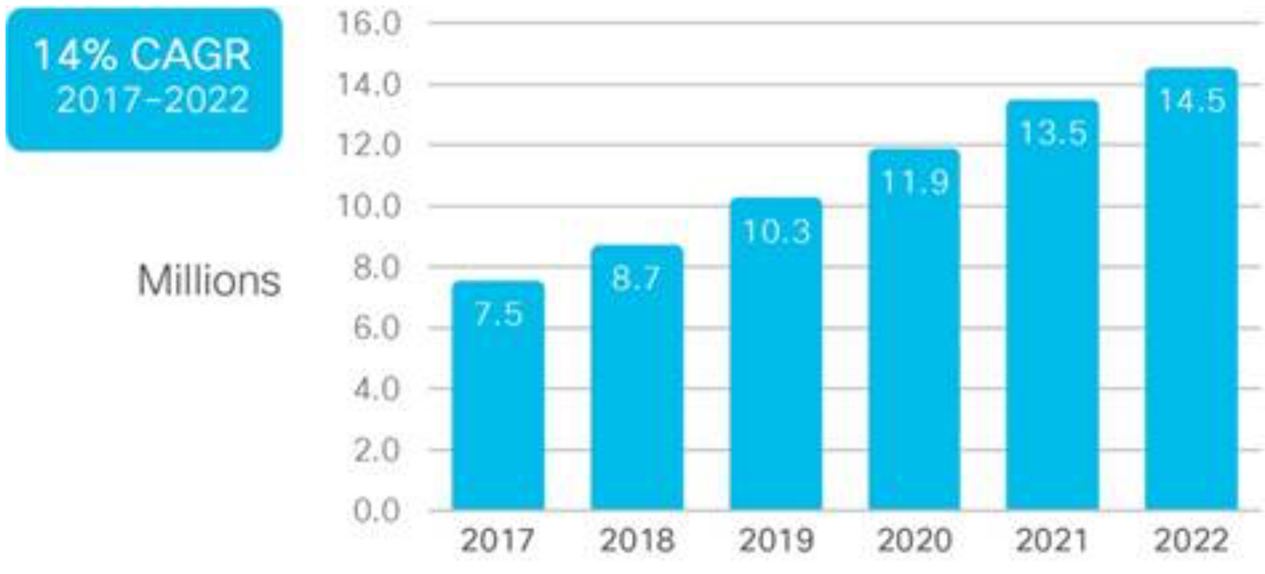
Distributed Denial of Service (DDoS) attacks



Traffic trace during the DDoS attack against DynDNS (2016)



Peak sizes of DDoS attacks (measured by Arbor Networks)



Source: Cisco VNI Global IP Traffic Forecast, 2017–2022

Cisco forecast of number of DDoS attacks

Some (more or less famous) relevant cyberattacks

1988 : Morris worm
First DDoS attack, ~6000 computers affected (10% Internet devices at the time), ~100M USD damage

1999 : Melissa
Virus spread as mail attachment, using MS-Office to propagate, 80M USD damage

1999 : NASA & DoD hacks
By teenager Jonathan James, 40K USD damage

2000 : Mafiaboy
DDoS attack against Amazon, eBay, Yahoo!, ~1200M USD damage

2002 : DNS root attacks
1 hour DDoS attack against the 13 root servers of DNS

2013 : Yahoo!
Attacks on Yahoo!, 500M and 1000M accounts compromised

2014 : Google DNS 8.8.8.8
BGP attack against 8.8.8.8: traffic re-routed towards Venezuela, Brazil

2015, 16 : AshleyMadison, AdultFriendFinder attacks
60 GB of account information and 400M accounts compromised, respectively. Poor password protection (SHA-1).

2016 : DynDNS attack
DDoS attack affecting Dyn's clients such as GitHub, Twitter, Spotify, Paypal, etc. Hacked IOT devices (~50K in 164 countries), infected by Mirai malware, used as "zombie armies". Traffic peaks of 280 Gbps

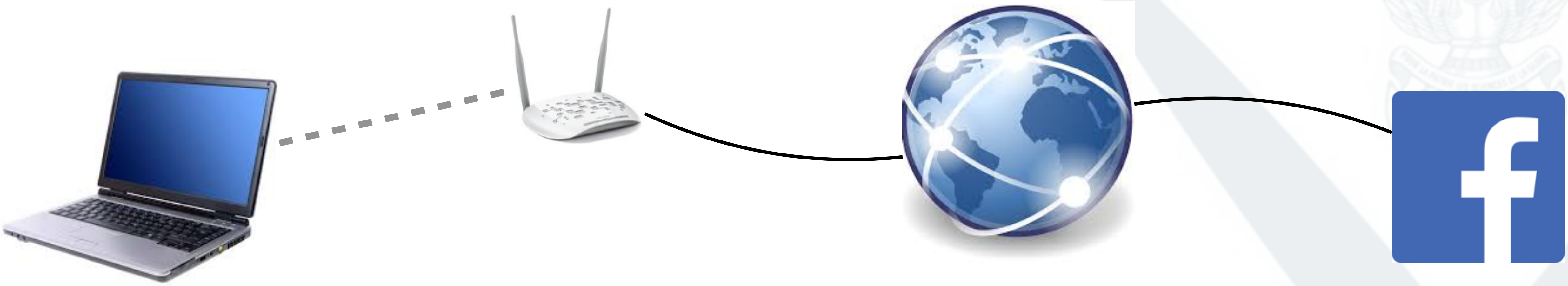
2018 : WannaCry
Ransonware attack (NHS, Telefonica, FedEx, etc.) exploiting MS SMB protocol vulnerability in Windows, 100 countries affected, 4000M USD damage estimated

What is DNS and why does it matter ?

Sources: https://www.gomindsight.com/blog/history-of-cyber-attacks-2018/, https://www.arnnet.com.au/slideshow/341113/top-10-most-notorious-cyber-attacks-history/, https://thehackernews.com/2014/03/google-public-dns-server-traffic.html

How does the Internet work : user's perspective

(user already connected to the Internet)



- User types "www.facebook.com" in his/her favourite browser

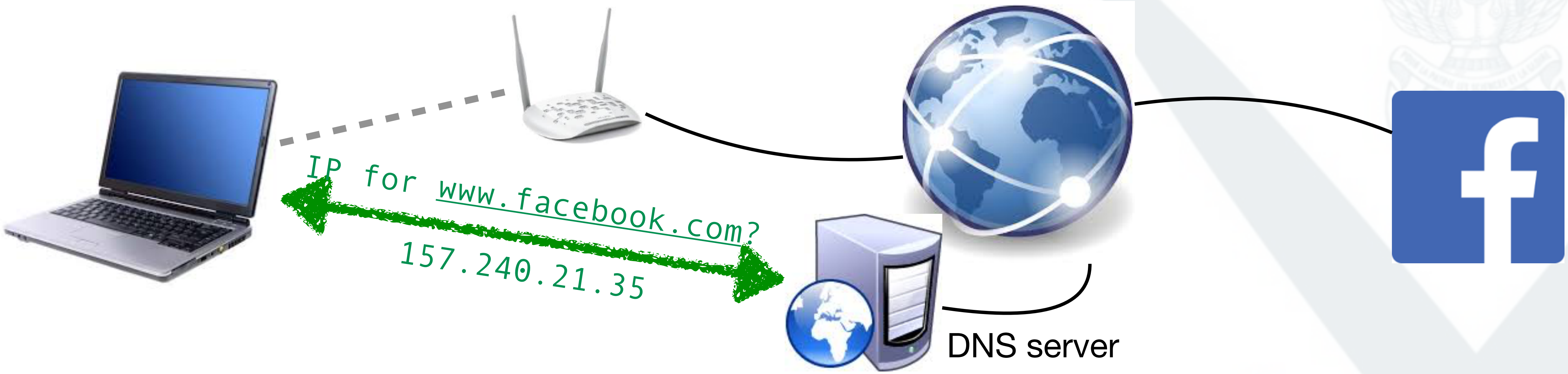
- What IP address corresponds to the domain name "www.facebook.com" ?
  => DNS query sent to the DNS server

- DNS replies with Facebook's IP address

- How to reach this IP address ?
  => Device routing table indicates *where* to send request (interface, gateway)

- Ready to go ! Send request, receive reply, etc.
  => Connection establishment and exchange (transport)

How does the Internet work : user's perspective



- User types "www.facebook.com" in his/her favourite browser

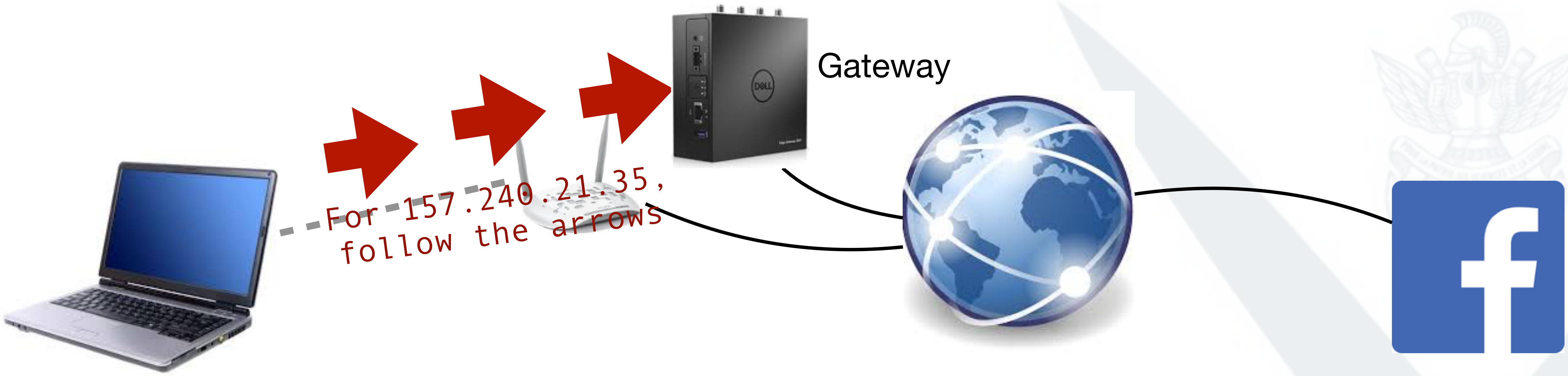
- What IP address corresponds to the domain name "www.facebook.com" ?
  => DNS query sent to the DNS server

- DNS replies with Facebook's IP address

- How to reach this IP address ?
  => Device routing table indicates *where* to send request (interface, gateway)

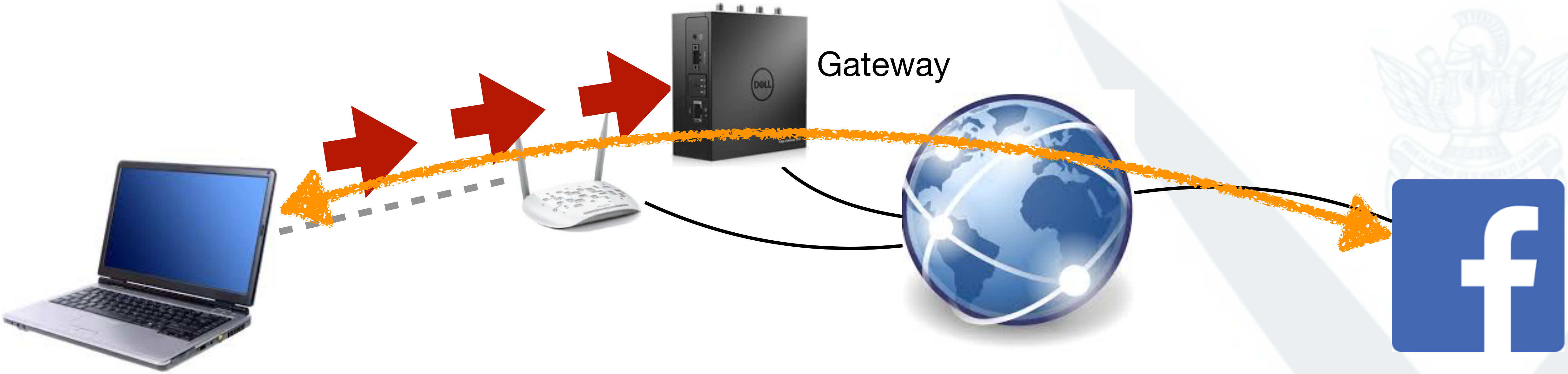
- Ready to go ! Send request, receive reply, etc.
  => Connection establishment and exchange (transport)

How does the Internet work : user’s perspective



- User types “www.facebook.com” in his/her favourite browser
- What IP address corresponds to the domain name “www.facebook.com” ?
  => DNS query sent to the DNS server
- DNS replies with Facebook’s IP address
- How to reach this IP address ?
  => Device routing table indicates *where* to send request (interface, gateway)
- Ready to go ! Send request, receive reply, etc.
  => Connection establishment and exchange (transport)

How does the Internet work : user’s perspective



- User types “www.facebook.com” in his/her favourite browser

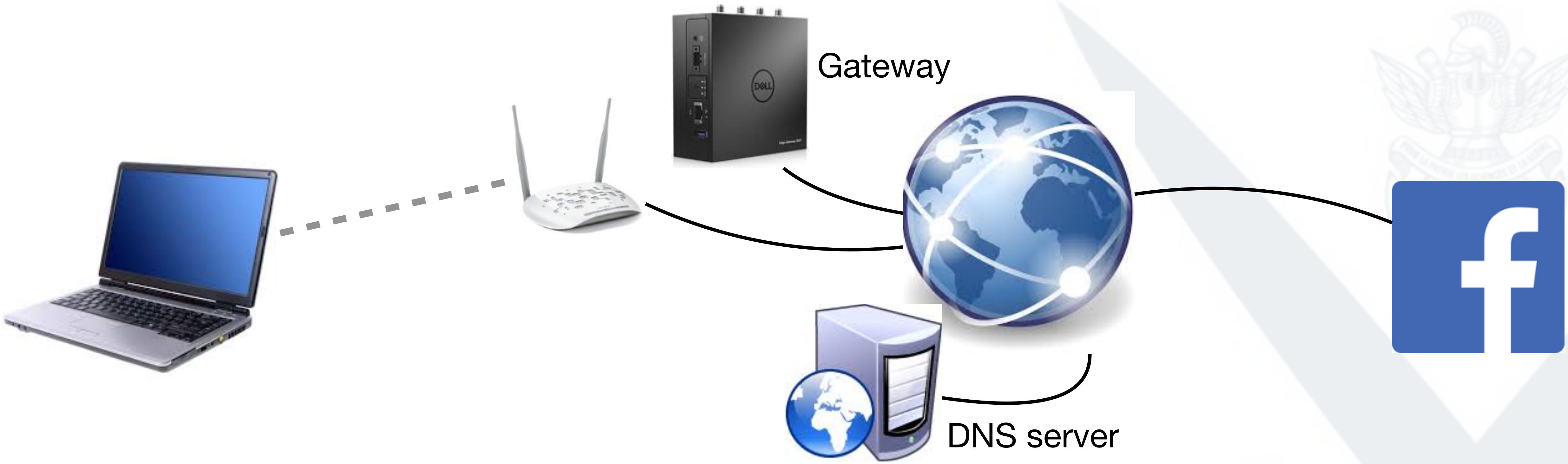
- What IP address corresponds to the domain name “www.facebook.com” ?
  => DNS query sent to the DNS server

- DNS replies with Facebook’s IP address

- How to reach this IP address ?
  => Device routing table indicates *where* to send request (interface, gateway)

- Ready to go ! Send request, receive reply, etc.
  => Connection establishment and exchange (transport)

How does the Internet work : user’s perspective



- User types “www.facebook.com” in his/her favourite browser

- What IP address corresponds to the domain name “www.facebook.com” ?
  => DNS query sent to the DNS server

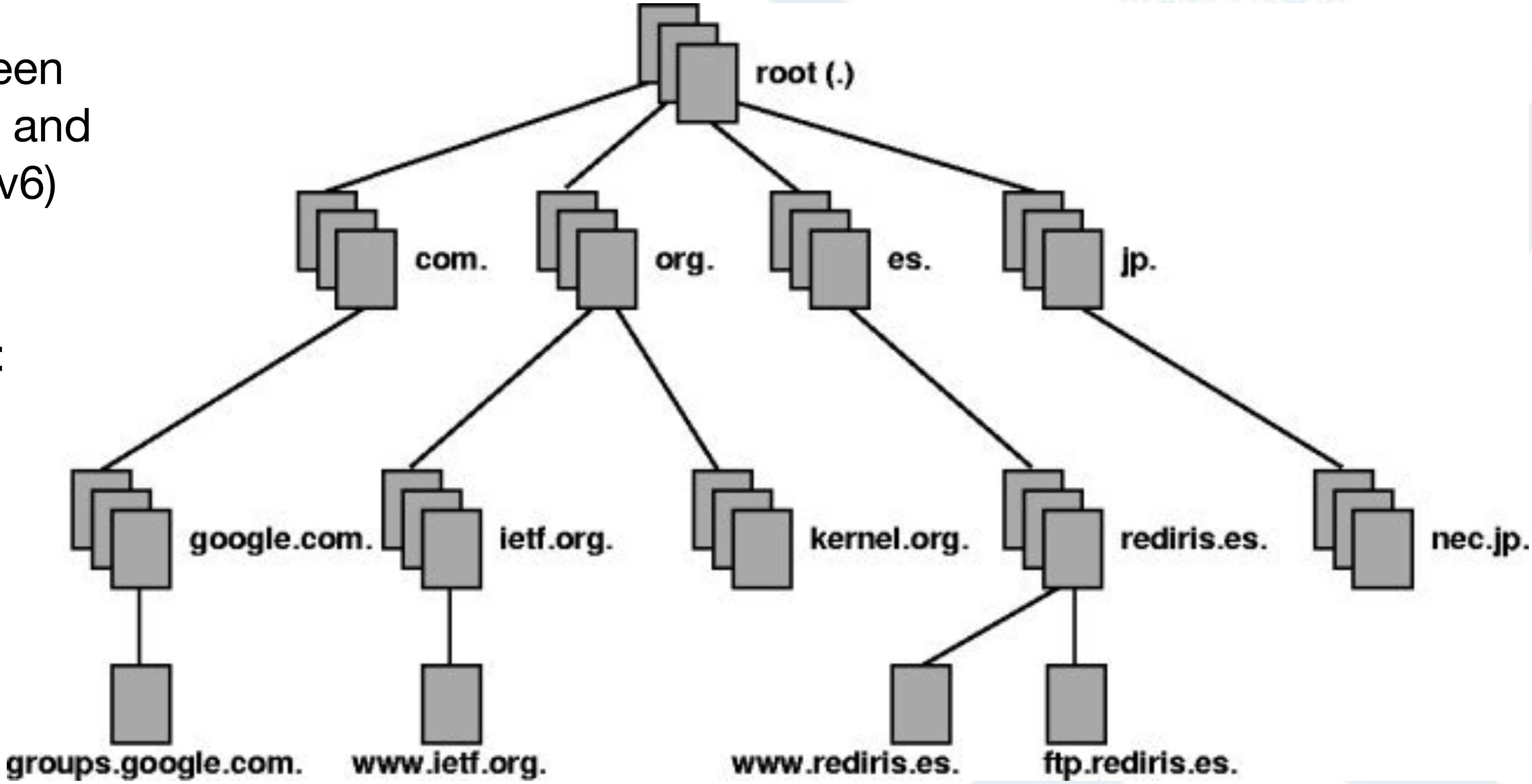
- DNS replies with Facebook’s IP address

- How to reach this IP address ?
  => Device routing table indicates *where* to send request (interface, gateway)

- Ready to go ! Send request, receive reply, etc.
  => Connection establishment and exchange (transport)

The Domain Name System (DNS)

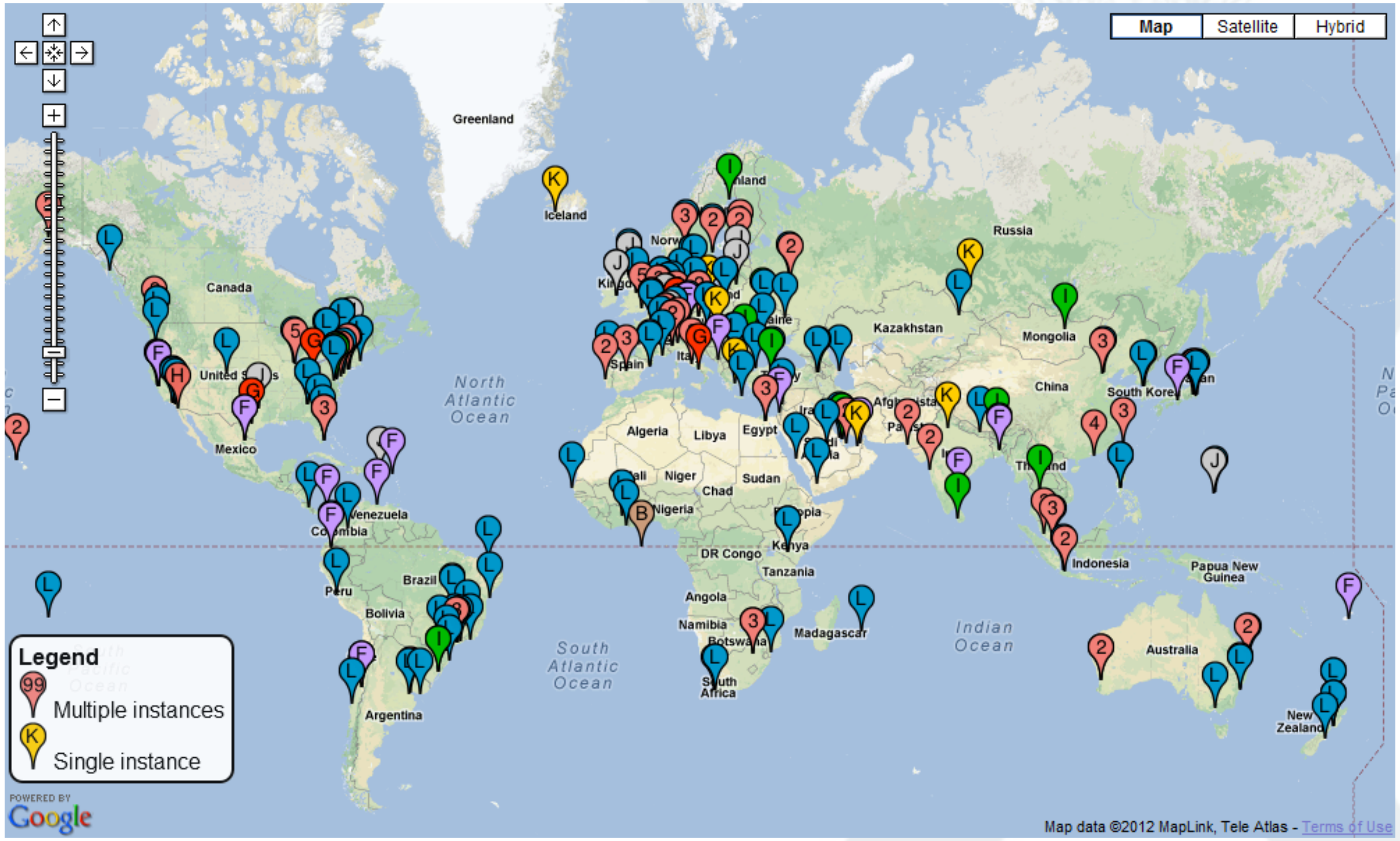
- A “global telephone book” for the Internet (1984)
  - Global mapping between domain names (URLs) and IP addresses (IPv4, IPv6)
  - Hierarchical database: on top, 13 distributed root servers, managed by ICANN
  - Distributed: many different DNS servers, ~10M resolvers, and way more caches (…including a “DNS cache” in your laptop)
  - Recursion: queries are either
    - replied, if known by the queried server, or
    - forwarded to a more authoritative server (“*someone who knows better*”), otherwise



The Domain Name System (DNS)

- A “global telephone book” for the Internet (1984)

  - Global mapping between domain names (URLs) and IP addresses (IPv4, IPv6)



  - Hierarchical database: on top, 13 distributed root servers, managed by ICANN

  - Distributed: many different DNS servers, ~10M resolvers, and way more caches (…including a “DNS cache” in your laptop)

  - Recursion: queries are either
    - replied, if known by the queried server, or
    - forwarded to a more authoritative server (“*someone who knows better*”), otherwise

The Domain Name System (DNS)

- Why DNS matters ?
  - If a domain name is not in DNS, ***it is not reachable***…
    (except you know its IP address !)

    Examples of IP addresses:
    157.240.21.35 (IPv4, 32 bits)
    fe80::d881:1dff:fe03:75c1 (IPv6, 128 bits)

    …it's pretty similar to "***it does not exist***"

The Domain Name System (DNS)

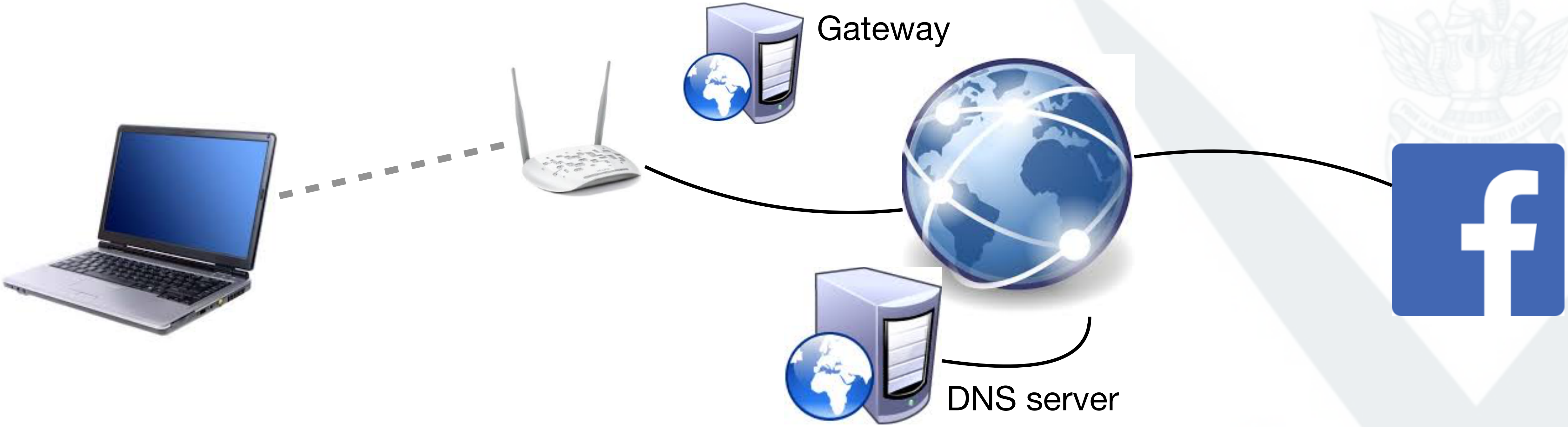
- Why DNS matters ?
  - If a domain name is not in DNS, ***it is not reachable***…
    (except you know its IP address !)

    Examples of IP addresses:
    157.240.21.35 (IPv4, 32 bits)
    fe80::d881:1dff:fe03:75c1 (IPv6, 128 bits)

    (…it's pretty similar to "***it does not exist***")

- Some ideas for DNS-based cyber attacks
  - What if a DNS server "learns" wrong mappings (DNS poisoning) ?
  - What if someone intercepts a DNS request, and replies pretending to be a legitimate DNS server ? (DNS spoofing)
  - …

How does the Internet work : user’s perspective



- User types “www.facebook.com” in his/her favourite browser

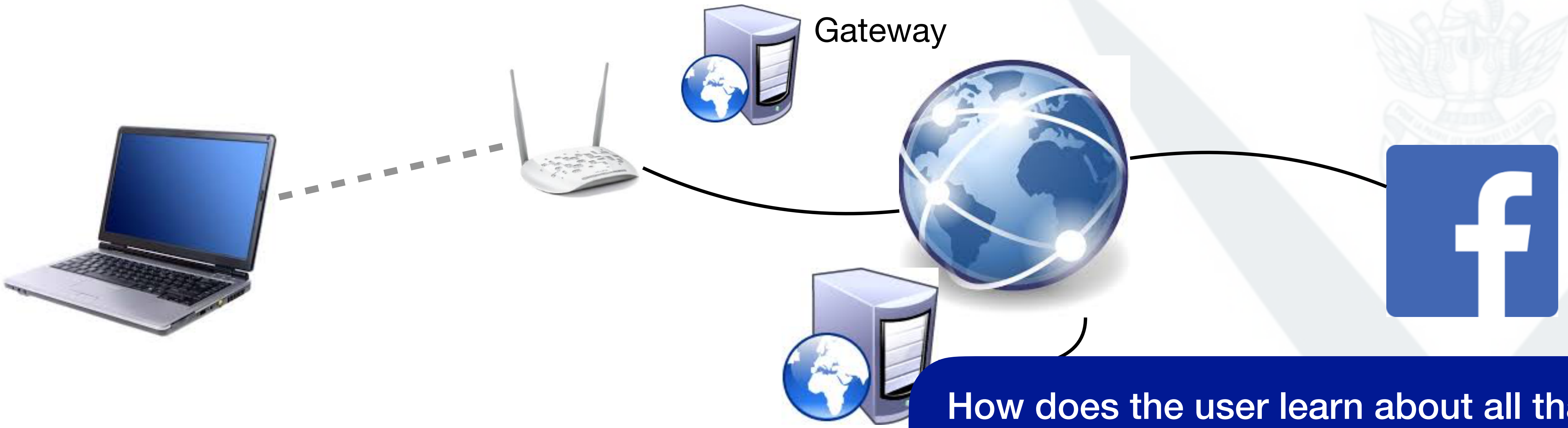
- What IP address corresponds to the domain name “www.facebook.com” ?
  => DNS query sent to the DNS server

- DNS replies with Facebook’s IP address

- How to reach this IP address ?
  => Device routing table indicates *where* to send request (interface, gateway)

- Ready to go ! Send request, receive reply, etc.
  => Connection establishment and exchange (transport)

How does the Internet work : user’s perspective



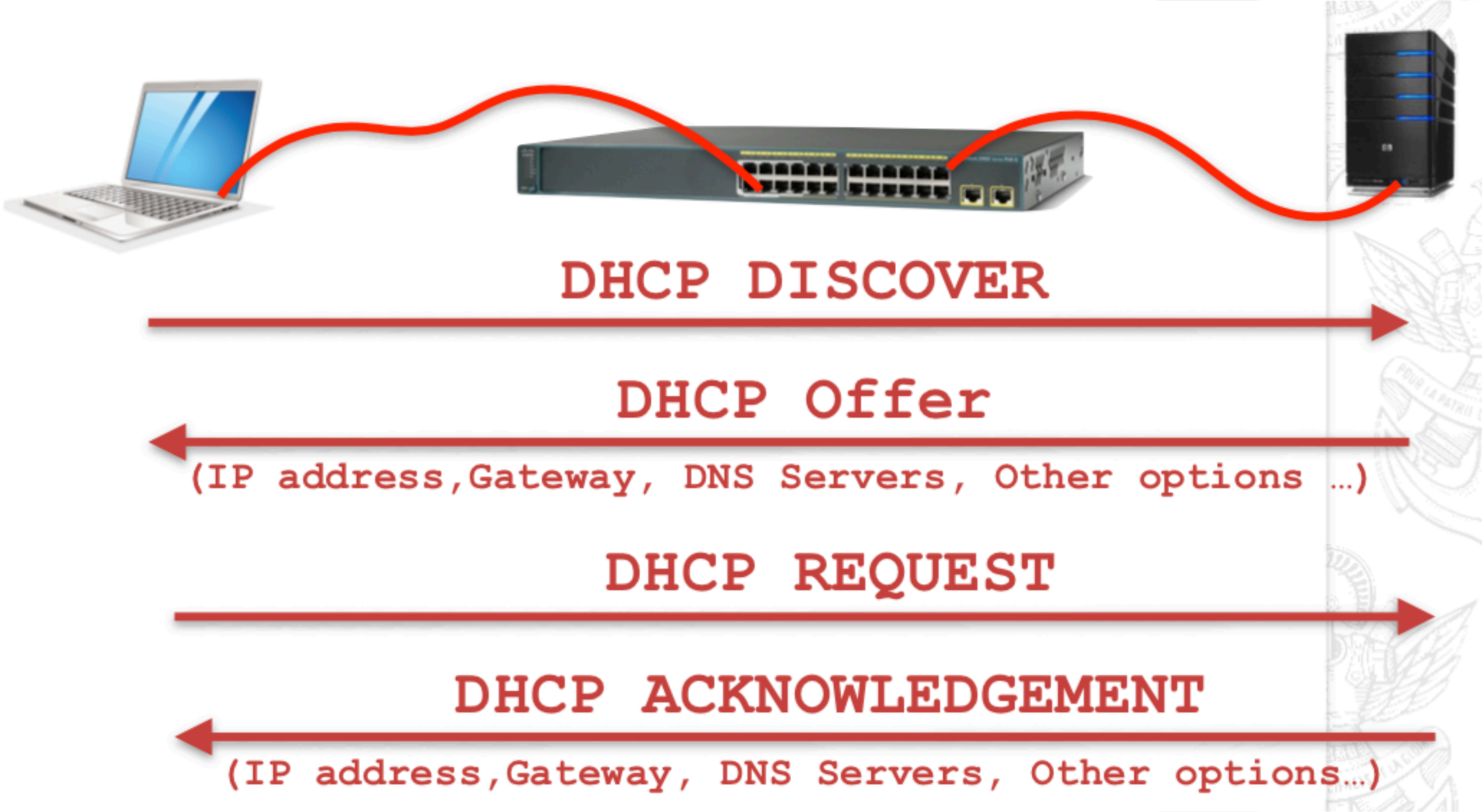
- User types “www.facebook.com” in his/her
- What IP address corresponds to the domai
  => DNS query sent to the DNS server
- DNS replies with Facebook’s IP address
- How to reach this IP address ?
  => Device routing table indicates *where* to send request (interface, gateway)
- Ready to go ! Send request, receive reply, etc.
  => Connection establishment and exchange (transport)

How does the user learn about all that is needed to connect to the Internet ?
(IP address, gateway, DNS server, routing table…)

This depends on the network.

How does the Internet work : user’s perspective

- DHCP : Dynamic Host Configuration Protocol



DHCP DISCOVER

DHCP Offer

(IP address,Gateway, DNS Servers, Other options …)

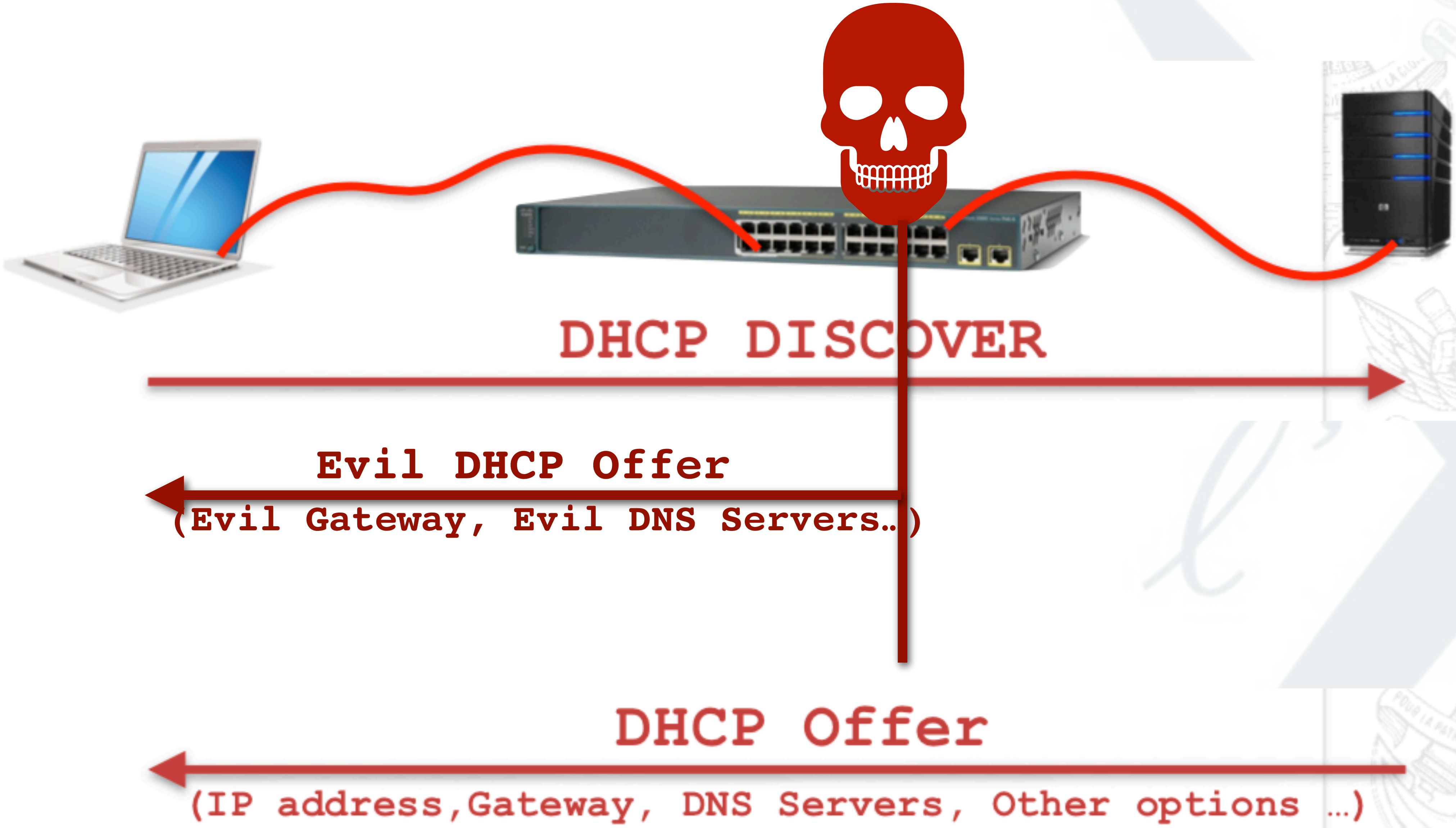
DHCP REQUEST

DHCP ACKNOWLEDGEMENT

(IP address,Gateway, DNS Servers, Other options…)

How does the Internet work : user’s perspective

- What if things go wrong… ?



DHCP DISCOVER

Evil DHCP Offer

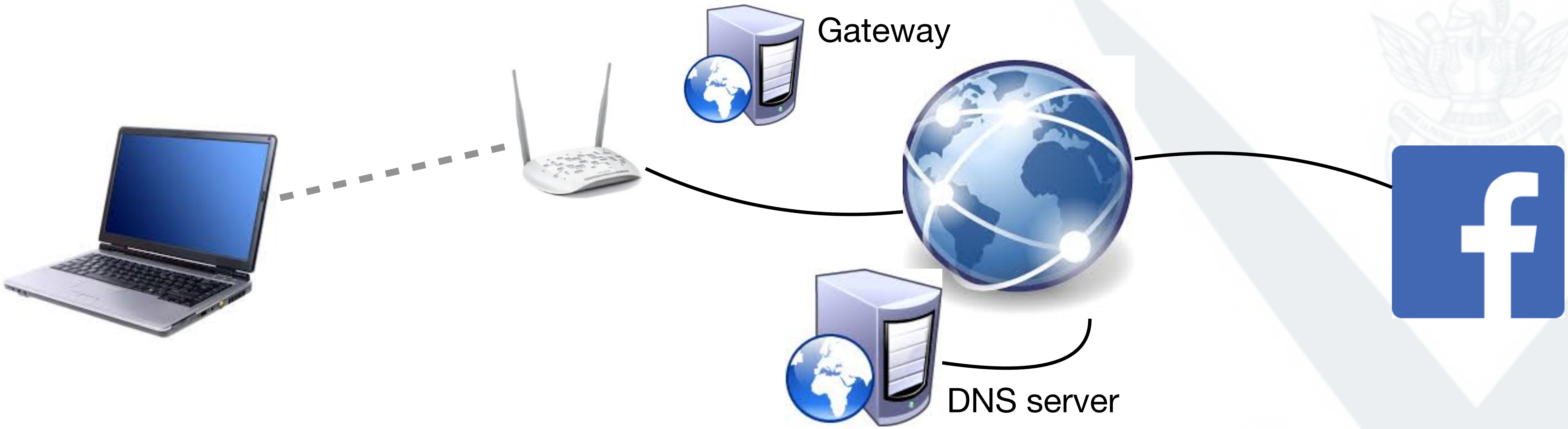
(Evil Gateway, Evil DNS Servers…)

DHCP Offer

(IP address,Gateway, DNS Servers, Other options …)

Man in the Middle (with DHCP spoofing)
User traffic can be re-routed to specific gateways, monitored, manipulated…

How does the Internet work : user’s perspective



- User types “www.facebook.com” in his/her favourite browser

- What IP address corresponds to the domain name “www.facebook.com” ?
  => DNS query sent to the DNS server

- DNS replies with Facebook’s IP address

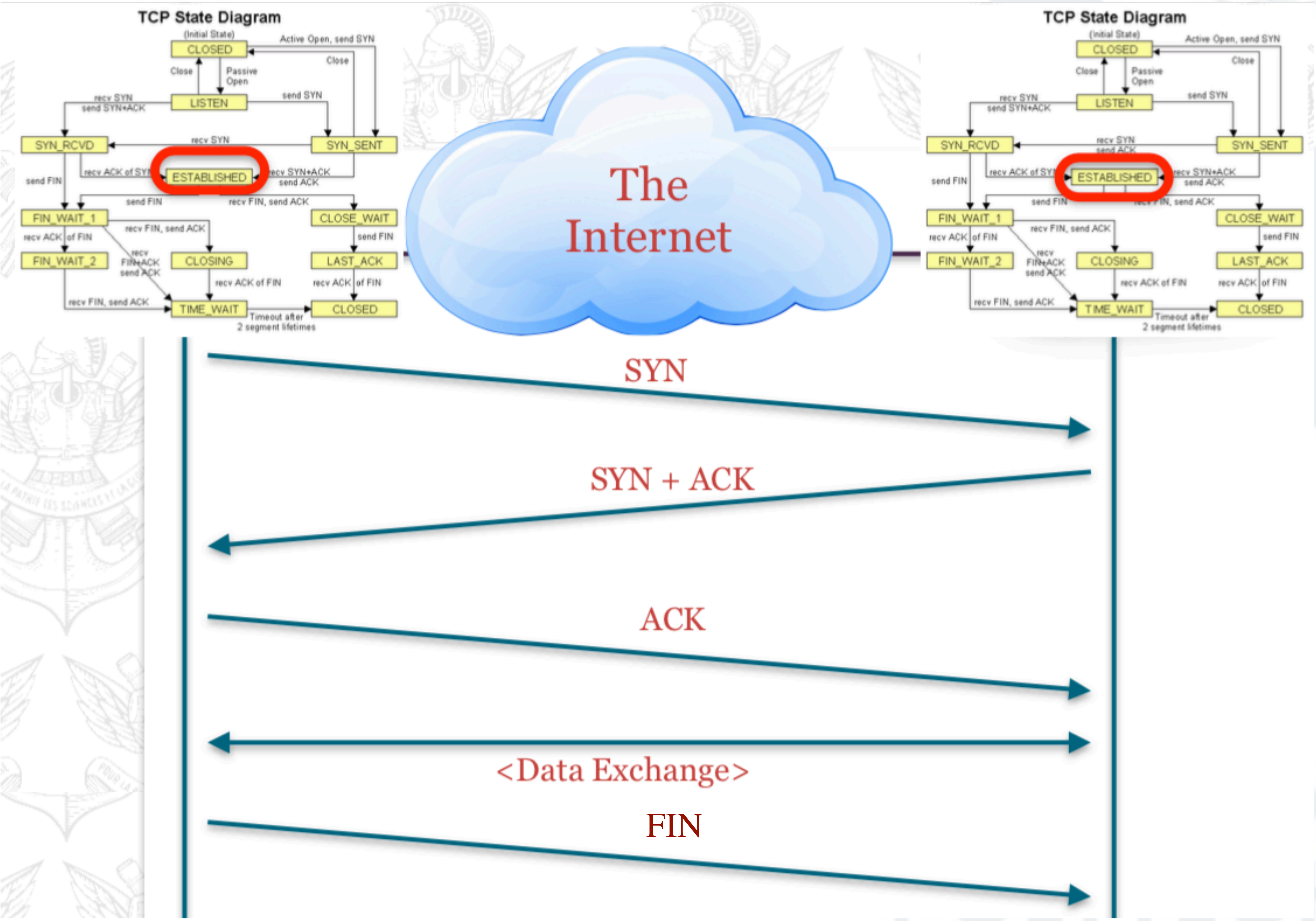
- How to reach this IP address ?
  => Device routing table indicates *where* to send request (interface, gateway)

- Ready to go ! Send request, receive reply, etc.
  => Connection establishment and exchange (transport)

How does the Internet work: user’s perspective

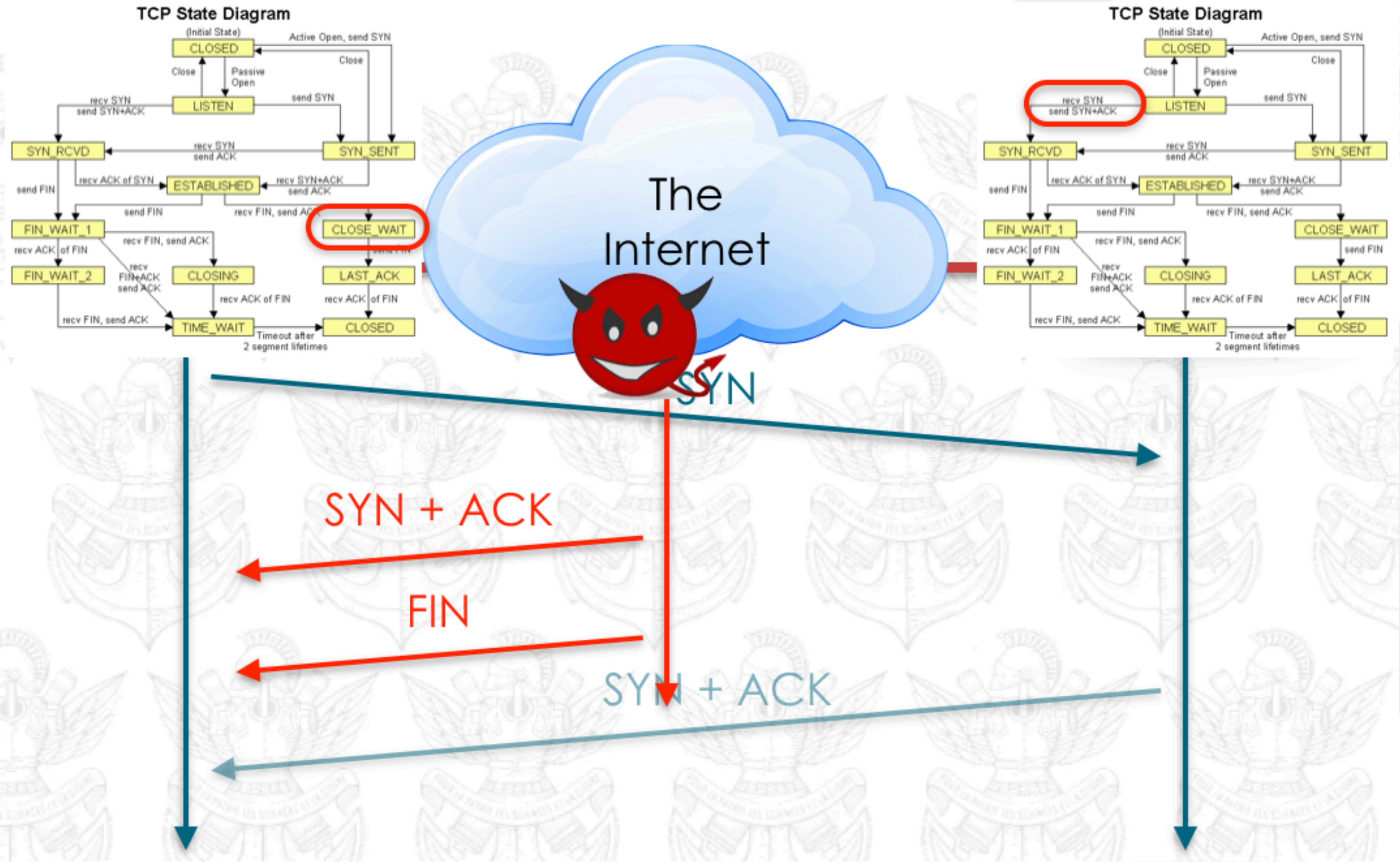
- **TCP** : Transport Control Protocol (1981)

- ~90% traffic of the Internet
- Provides “reliable” transport: if packets are lost, they are sent again



How does the Internet work: user’s perspective

- Attacking TCP



- TCP connection resetting

- But also: SYN attacks to servers for Denial of Service…

Is that sufficient to disrupt or shut down the Internet ?

- **China** Internet control model : *wang guan* (网管, net wall)
  - Some filtering techniques
    (source: https://www.howtogeek.com/162092/htg-explains-how-the-great-firewall-of-china-works/)

  - IP blacklists
  - URL filtering
  - Deep Packet Inspection over unencrypted packets
  - VPN blocking

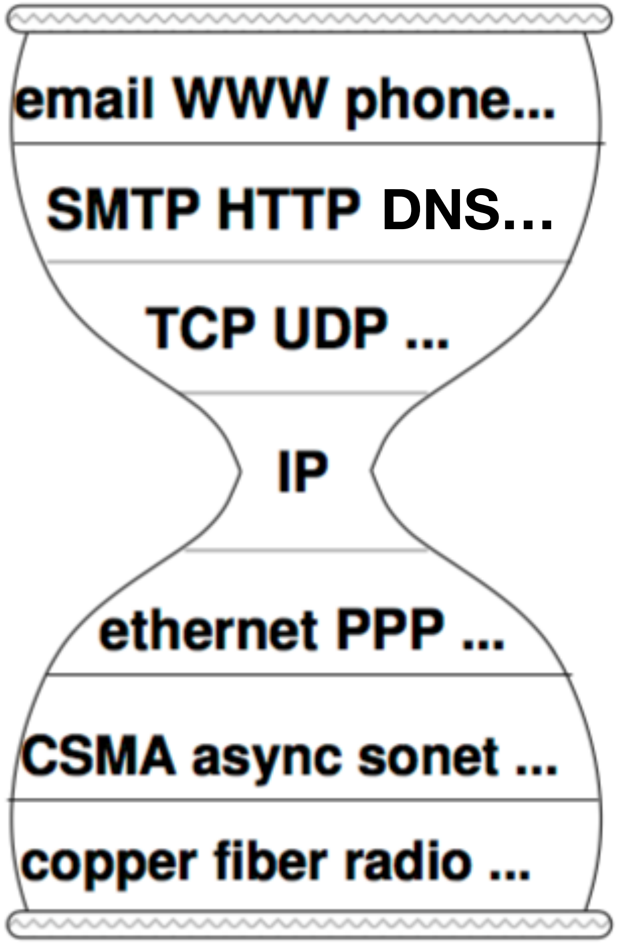
  - DNS Poisoning
  - TCP connections resetting

  - …and a lot of manpower

- No measure is ***totally*** effective… but they only need to be ***sufficiently*** effective !

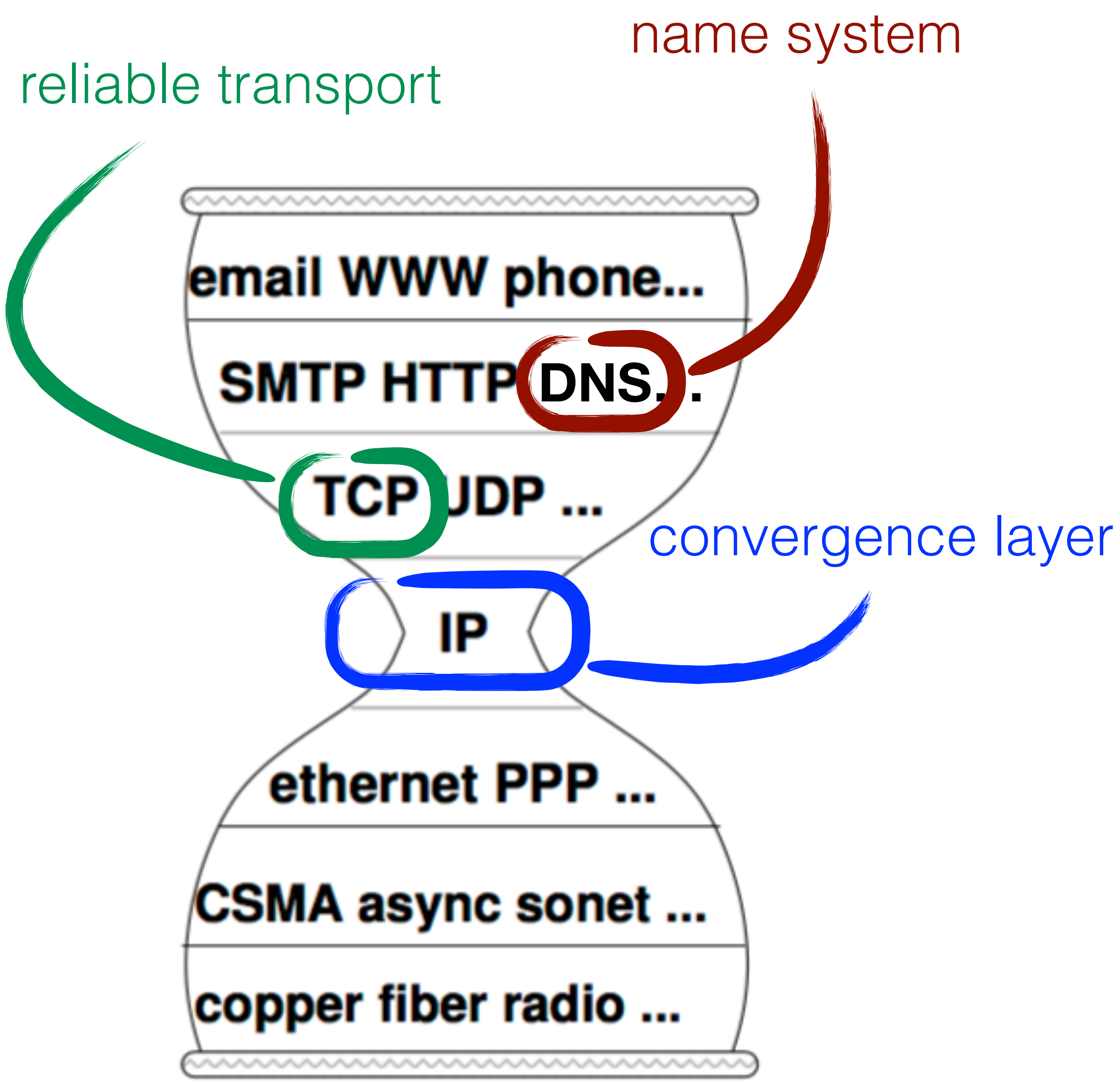
Internet inherent vulnerabilities

- TCP/IP protocol stack : “*the hourglass view*”



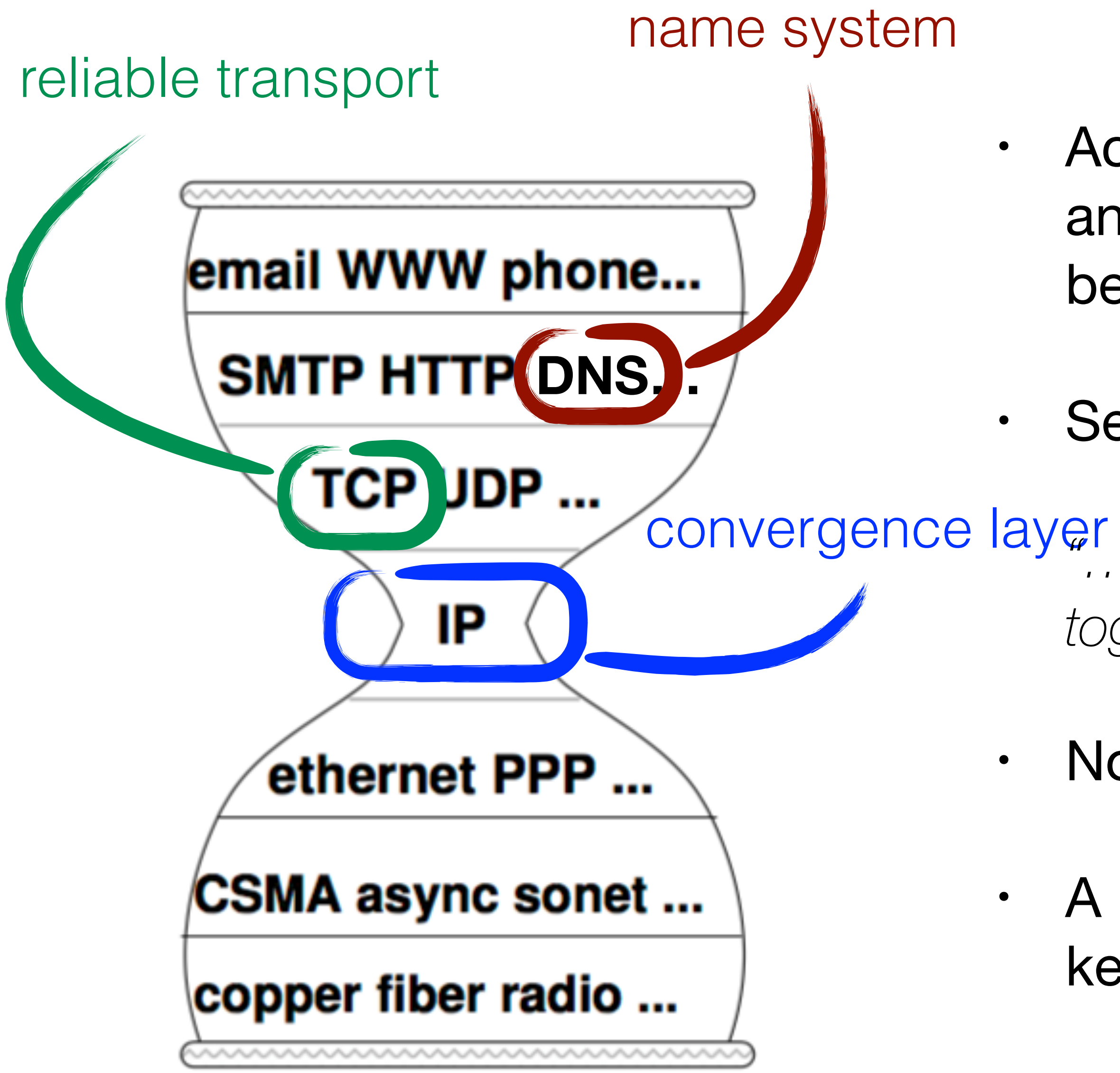
Internet inherent vulnerabilities

- TCP/IP protocol stack : “*the hourglass view*”



Internet inherent vulnerabilities

- TCP/IP protocol stack : "*the hourglass view*"



- Academic/research origin, **open** philosophy, initial users and devices were **trusted** => Protection against malicious behavior was not a priority

- Security was addressed in terms of **survivality**:

  "…the ability of the surviving stations [of the network] to operate together as a coherent entity after attack" (Baran, 1962)

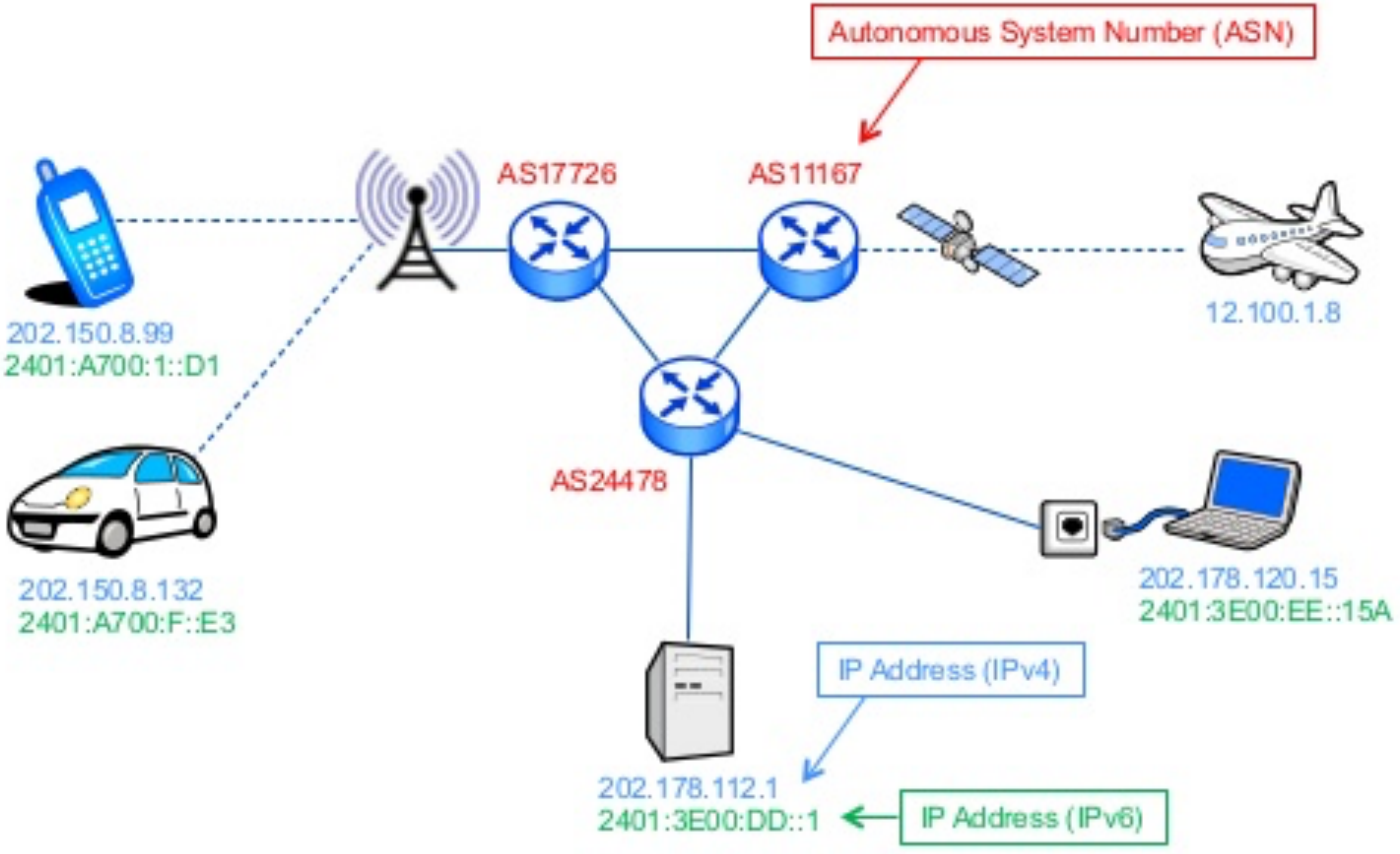
- Not designed to become *this* big

- A basic "Internet user experience" mobilizes some of the key protocols and exposes relevant vulnerabilities

- Security mechanisms (SSL/TLS, DNSSEC, VPN) have been developed *a posteriori*
  - *…but they don't touch the core !*

A macroscopic view of the Internet

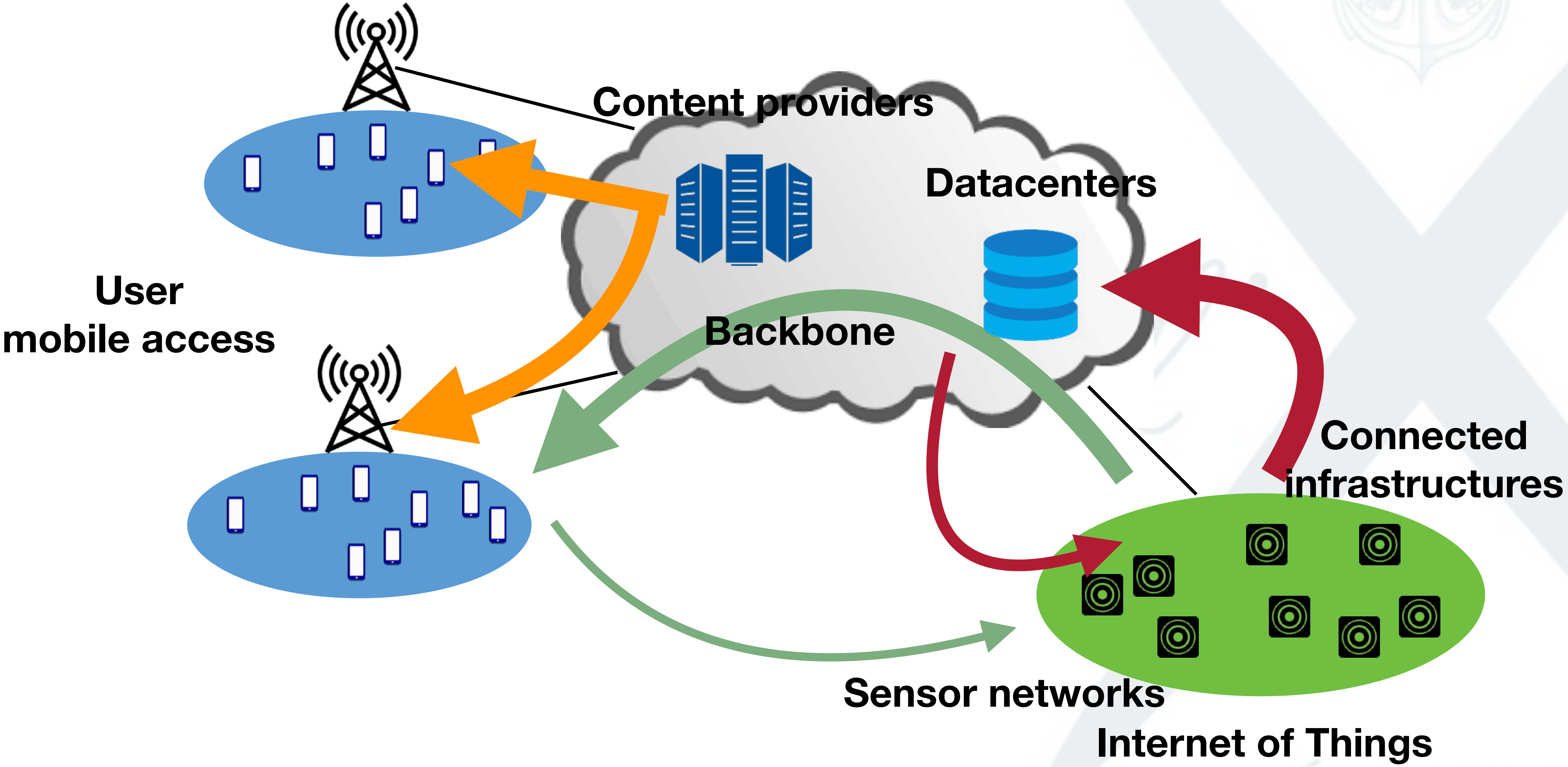
- A **core** and an **edge**



(Source: APNIC)

A macroscopic view of the Internet in a digitized society

- A (wired) **core** and a (increasingly wireless) **edge**



Wireless vulnerabilities

- Communications “in the air” are intrinsically open
  - Easier to listen to the (shared) medium than to tap a cable
- Additional protection required : you don’t know your “audience”
- High range / short range
- Technology-specific

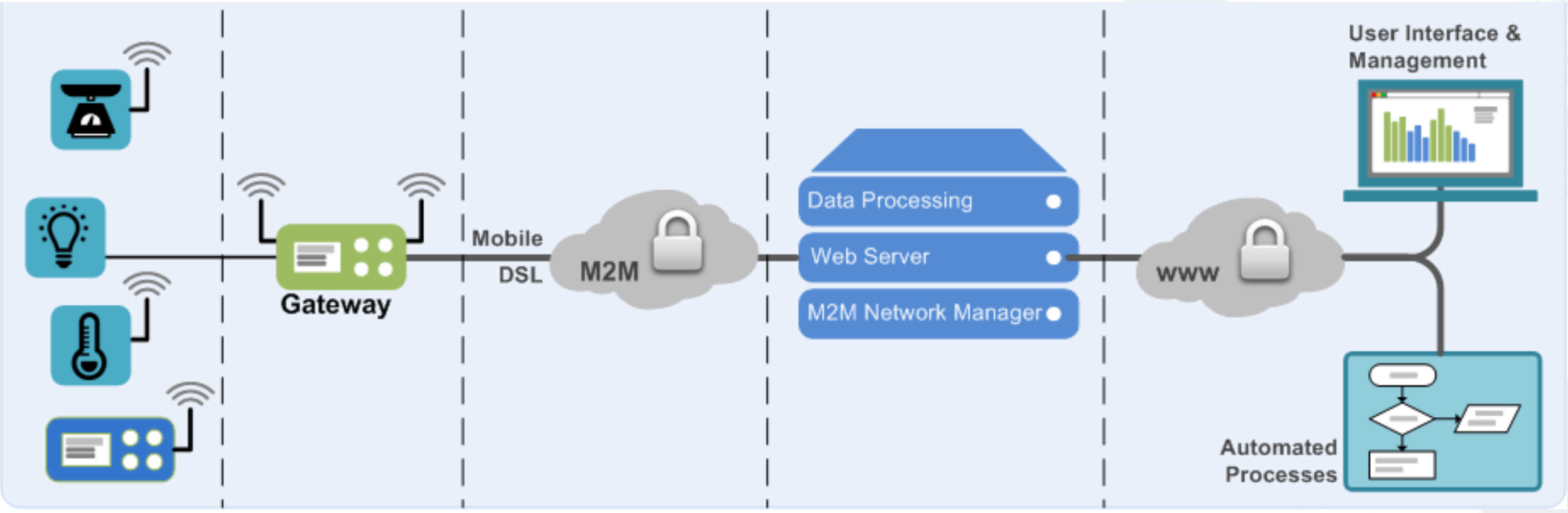
Wireless vulnerabilities

- Communications “in the air” are intrinsically open
  - Easier to listen to the (shared) medium than to tap a cable
- Additional protection required : you don’t know your “audience”
- High range / short range
- Technology-specific

- **Bluetooth**
  - Until BT2.0+EDR (2004), pairing required devices having the same PIN
  - PINs typically consisted of 4 digits (although they could be 16 bytes !)
  - Weaknesses known since 2001
- **Wi-Fi**
  - WEP, released in 1999, vulnerabilities exposed in 2001
    - Poor cryptographic design (not the algorithm itself)
    - Too-short keys
  - WPA/WPA2:
    - Vulnerability in the Wi-Fi Protected Setup (WPS) feature
    - Reaver (source: https://arstechnica.com/information-technology/2011/12/researchers-publish-open-source-tool-for-hacking-wifi-protected-setup/)

Wireless vulnerabilities

- Wireless technologies for the **IoT**



Typical IoT architecture

sigfox

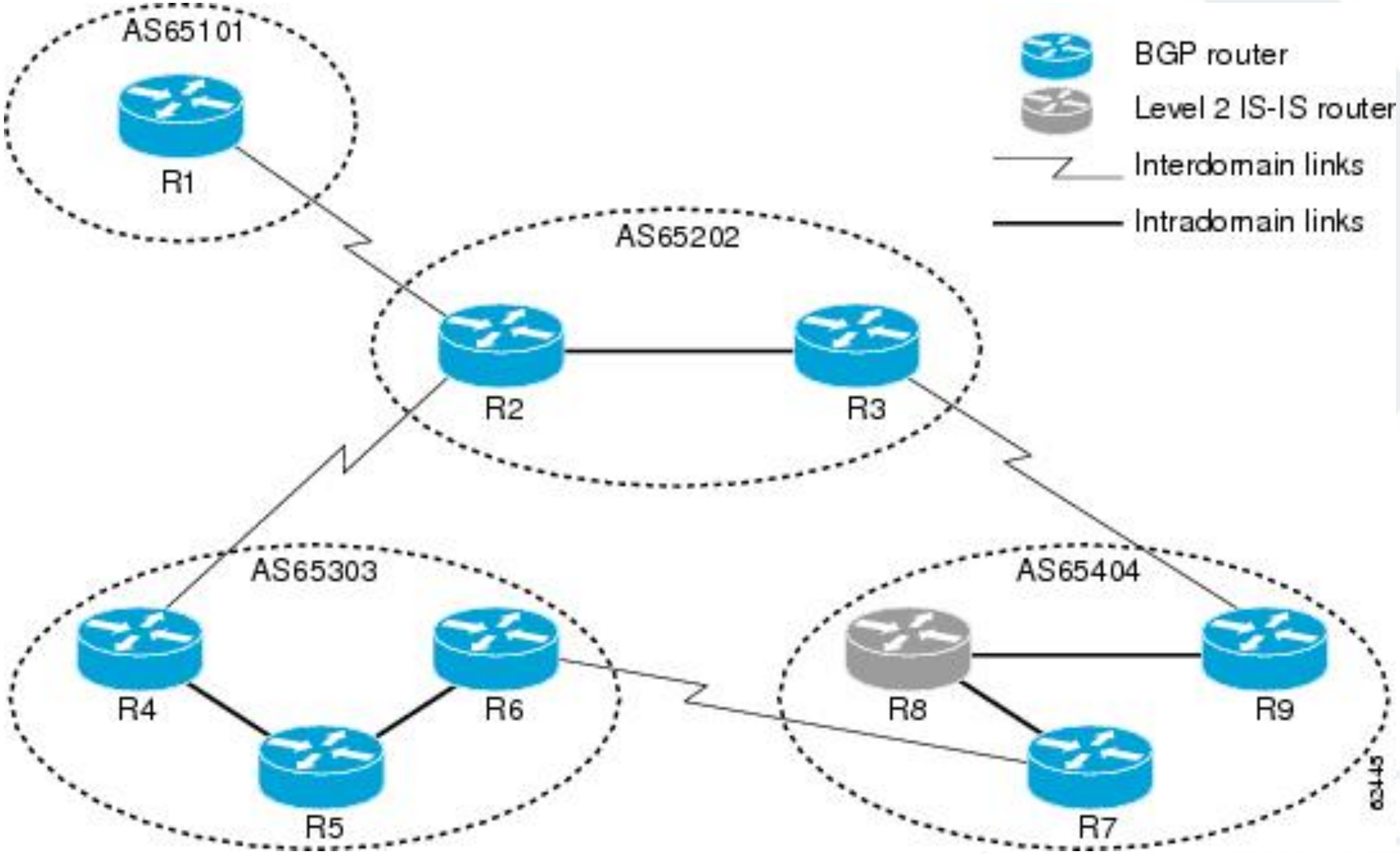
ZigBee

LoRa

- Long range (**LoRa**, **Sigfox**), short range (**Zigbee**, 802.15.4…)
- Heavily constrained devices, low-capacity communication channels
  => security mechanisms (signatures, encryption, decryption, long keys…) are **costly**
- Even if their use is not deemed critical, vulnerabilities may turn them dangerous (e.g. **botnets**)

A macroscopic view of the Internet: the (wired) core

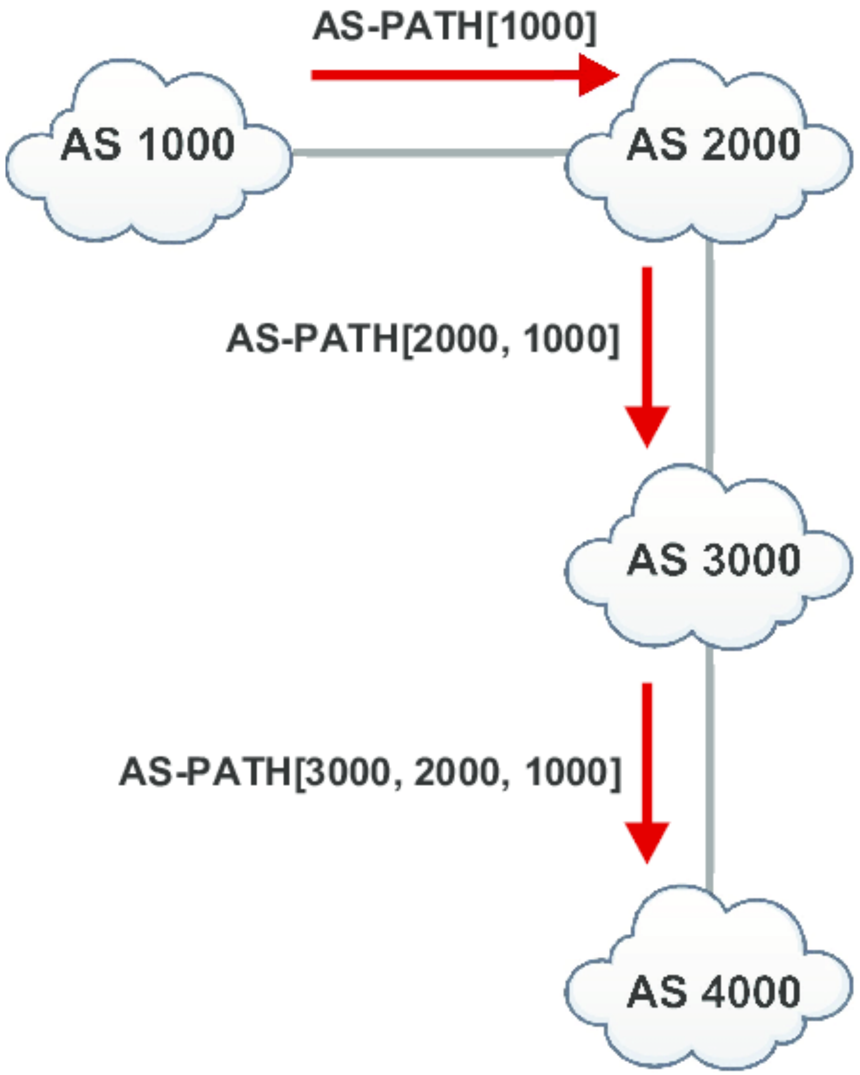
- *Logically*, the Internet is a network of networks, each (inter)network being operated independently
  - Autonomous Systems (ASs) : collection of networks under the same authority
  - ~ 63K ASes (source: cidr-report.org)
  - ASes coordinated for routing through BGP

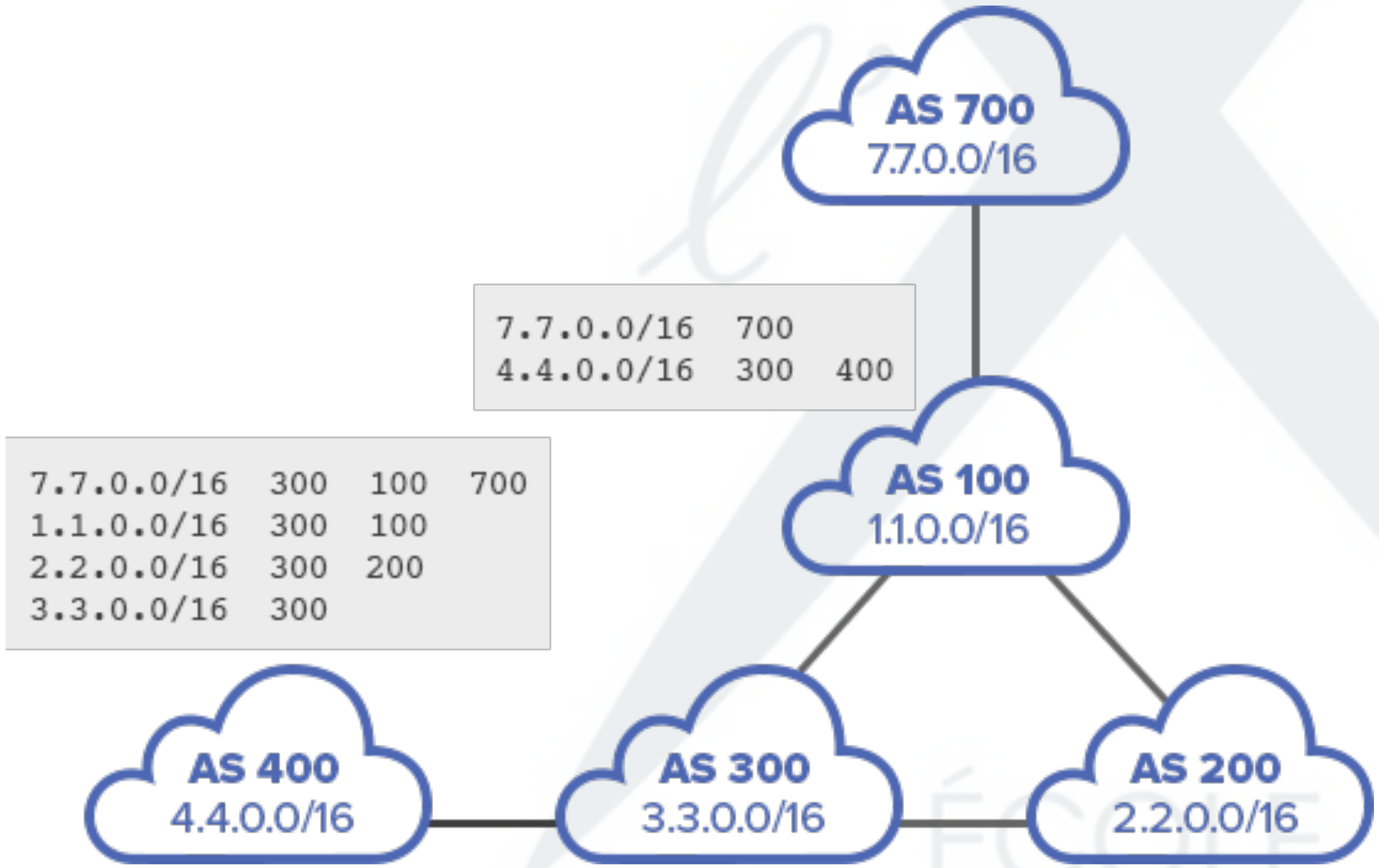


Source: Cisco Systems

A word on BGP

- Border Gateway Protocol (1994) : "*the protocol that makes the Internet work*"
  - Routing protocol : each AS (*peer*) announces the networks that are reachable through it
  - …networks not being announced (or withdrawn from BGP updates) are ***not reachable*** outside their AS
  - Consistency and stability of BGP routing tables are <u>major issues</u> in the Internet





```
7.7.0.0/16   700
4.4.0.0/16   300   400
```

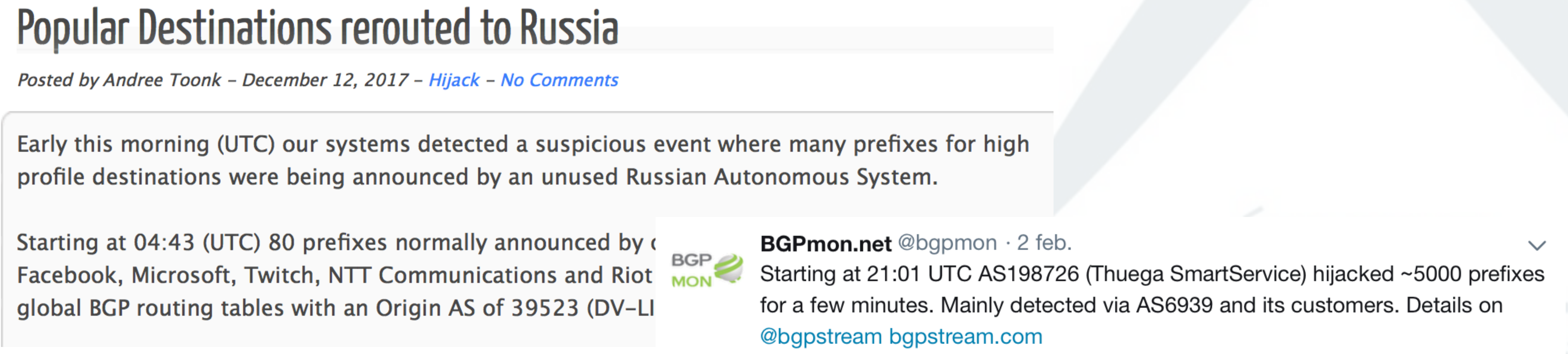
```
7.7.0.0/16   300   100   700
1.1.0.0/16   300   100
2.2.0.0/16   300   200
3.3.0.0/16   300
```

A word on BGP

- Border Gateway Protocol (1994) : “*the protocol that makes the Internet work*”
    - …again, relying on the *bona fide* of peers
    - Malicious BGP updates/claims (or errors due to misconfiguration !) can have a substantial impact in terms of traffic (re-routing…) and be used for DoS/DDoS purposes
    - Security extensions designed (BGPSEC), but not fully deployed

2014 : Google DNS 8.8.8.8
BGP attack against 8.8.8.8: traffic re-routed towards Venezuela, Brazil

> “While BGP plays a crucial role in Internet communications, it remains **surprisingly vulnerable to attack**. The past few years have seen a range of routing incidents (..) from a simple misconfiguration at a small Indonesian ISP that took Google offline in parts of Asia, to a case of BGP-based censorship that leaked out of Pakistan Telecom and took YouTube offline for most of the Internet, to a routing error that caused a large fraction of the world’s Internet traffic to be routed through China Telecom, to highly targeted traffic interception by networks in Iceland and Belarus…”
>
> (ACM Queue, Sept. 2014, https://queue.acm.org/detail.cfm?id=2668966)



Popular Destinations rerouted to Russia

Posted by Andree Toonk – December 12, 2017 – Hijack – No Comments

Early this morning (UTC) our systems detected a suspicious event where many prefixes for high profile destinations were being announced by an unused Russian Autonomous System.

Starting at 04:43 (UTC) 80 prefixes normally announced by
Facebook, Microsoft, Twitch, NTT Communications and Riot
global BGP routing tables with an Origin AS of 39523 (DV-LI

BGPmon.net @bgpmon · 2 feb.
Starting at 21:01 UTC AS198726 (Thuega SmartService) hijacked ~5000 prefixes for a few minutes. Mainly detected via AS6939 and its customers. Details on @bgpstream bgpstream.com

A macroscopic view of the Internet : the (wired) core

- *Physically*, the Internet is a set of **(mostly undersea) cables**…

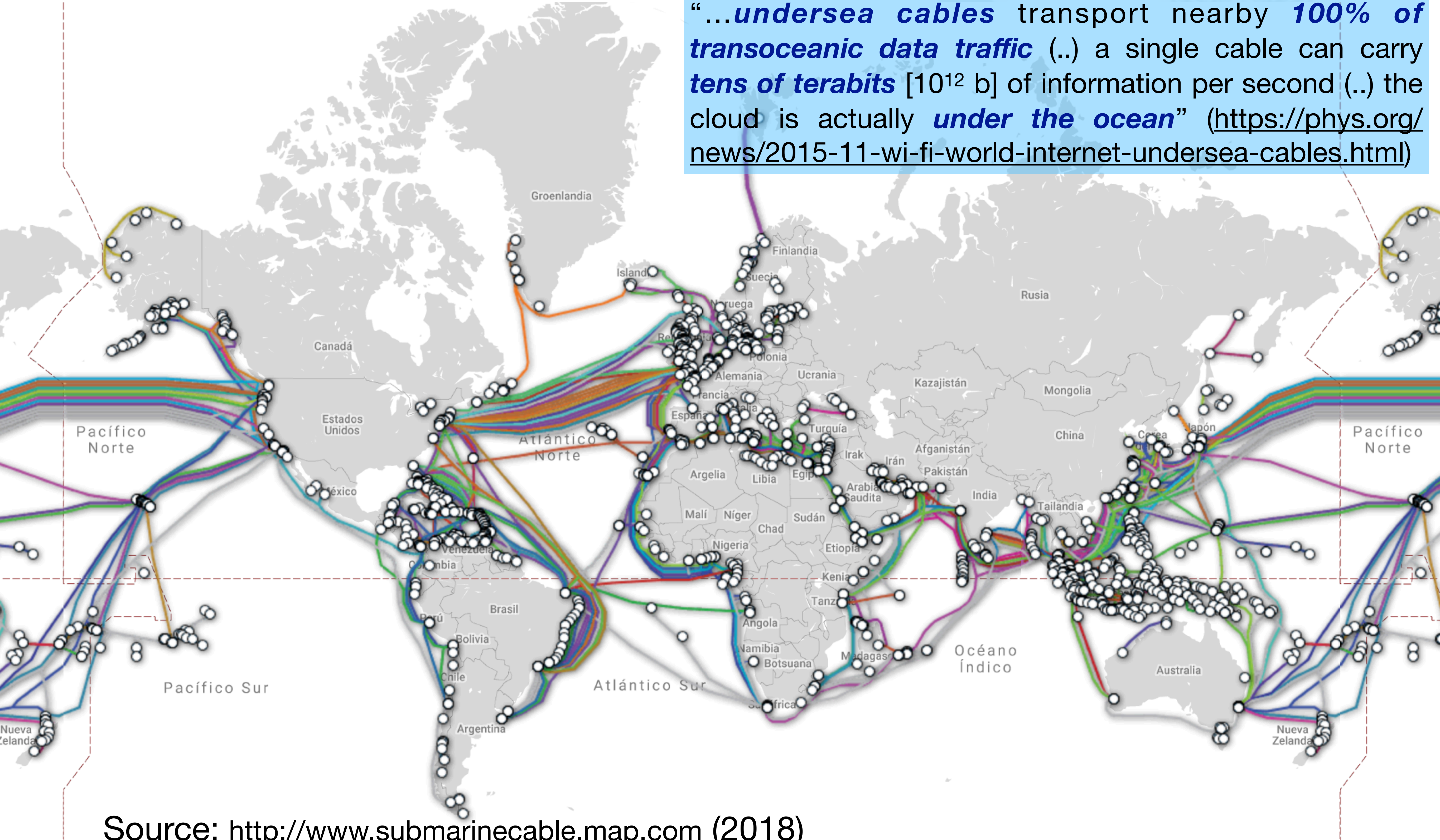
“*…there are a little* ***over 200 systems*** *that carry all of the internet traffic across the ocean, and these are by and large concentrated in* ***very few areas****. The cables end up getting funneled through these narrow pressure points all around the globe.*” (Nicole Stariolevski, author of The Undersea Network)

(source: https://www.wired.com/2015/10/undersea-cable-maps/)

Internet submarine cable map

- *Physically*, the Internet is a set of **(mostly undersea) cables**…

“…***undersea cables*** transport nearby ***100% of transoceanic data traffic*** (..) a single cable can carry ***tens of terabits*** [10^{12} b] of information per second (..) the cloud is actually ***under the ocean***” (https://phys.org/news/2015-11-wi-fi-world-internet-undersea-cables.html)

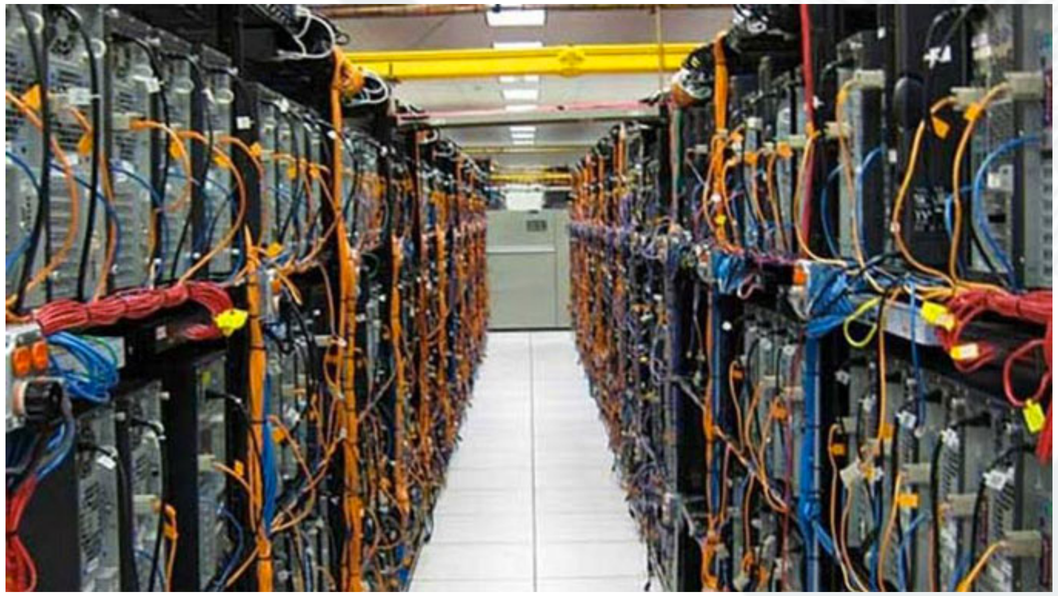


Source: http://www.submarinecable.map.com (2018)

A macroscopic view of the Internet : the (wired) core

- *Physically*, the Internet is a set of **(mostly undersea) cables**…

- …meeting at large interconnection facilities (**IXPs**)



Internet Exchange Point (IXP) in Morocco

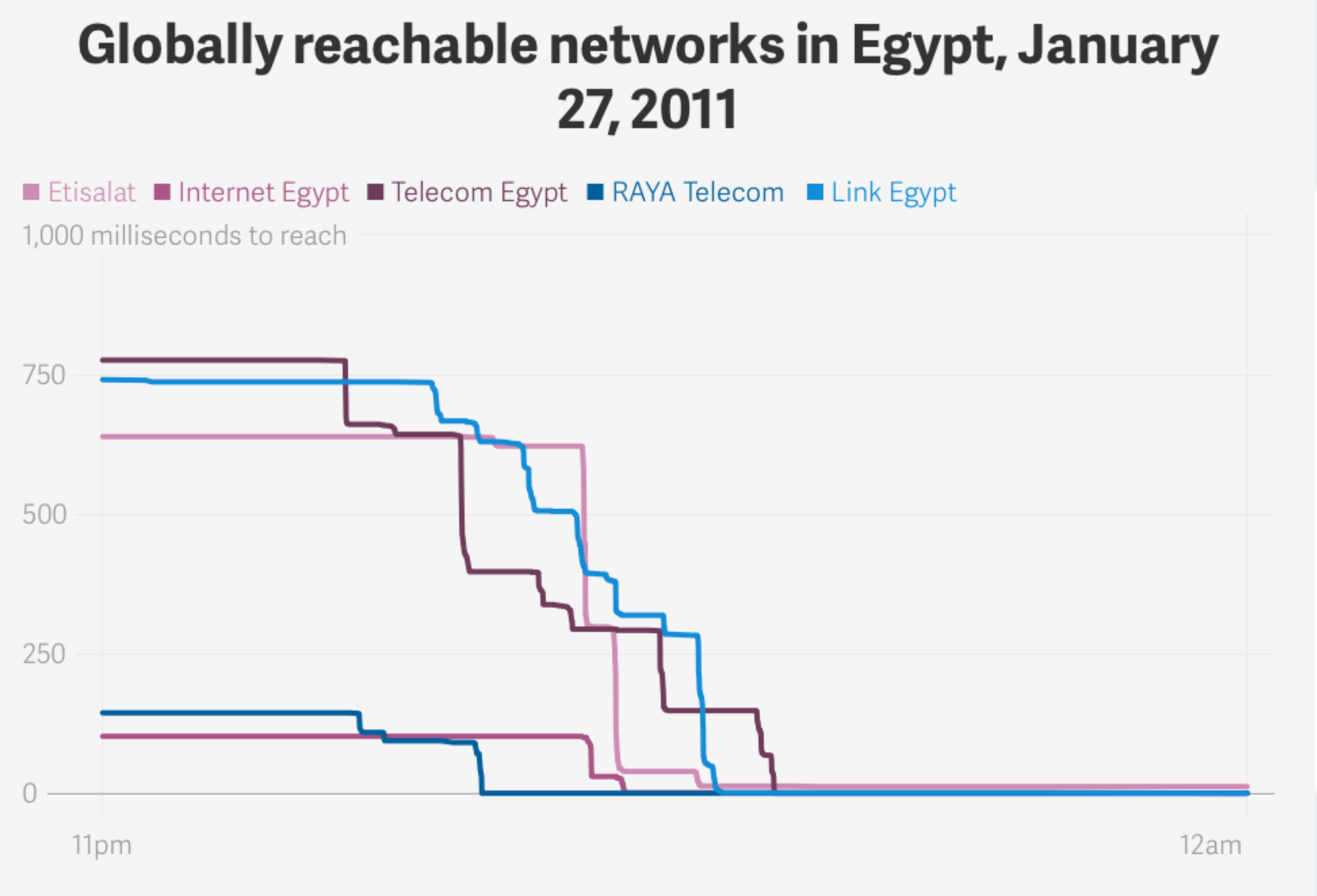
- …and flowing traffic from/to a **few** (and decreasing!) number of poles

Facebook data center, Des Moines, Iowa, US

Google data center, The Dalles, Oregon, US

Is it possible to shut down the Internet ?

- Arab springs (2011): the case of **Egypt**
  - DNS filtering
  - Internet disconnection (BGP route withdrawing)
    - Either through instructions to ISPs, or through physical disconnection at the Cairo Regional Internet Exchange (CAIX)

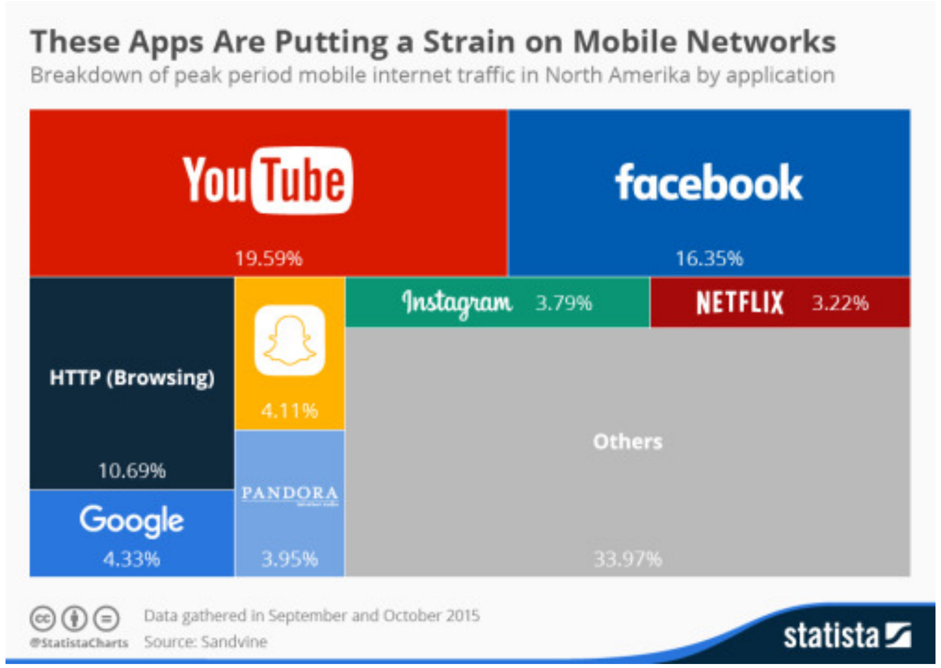


Source: https://www.theatlas.com/charts/H1wgJeJa

- Traffic anomalies in the Internet (due to misconfigurations or malicious attacks) happening quite frequently (~hundreds/month).
  - (source: https://securityintelligence.com/bgp-internet-routing-what-are-the-threats/)

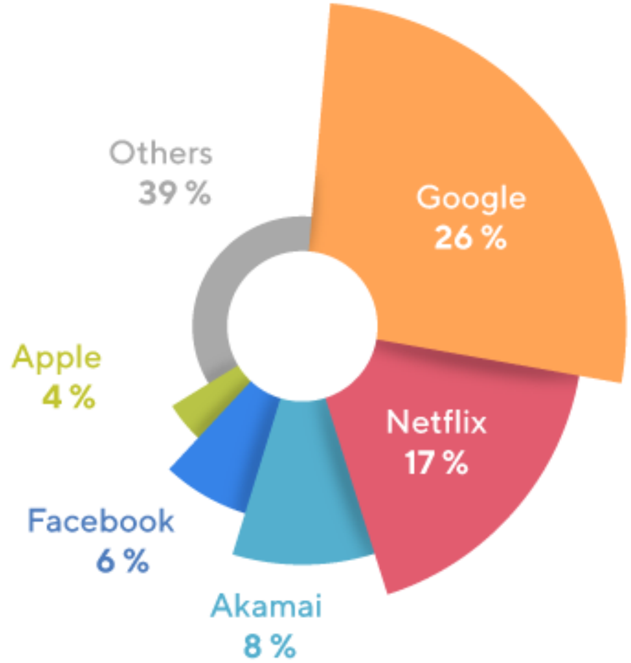
Other ongoing trends

- **Centralization** (in usage, in technologies, in hardware, in CDN usage…)

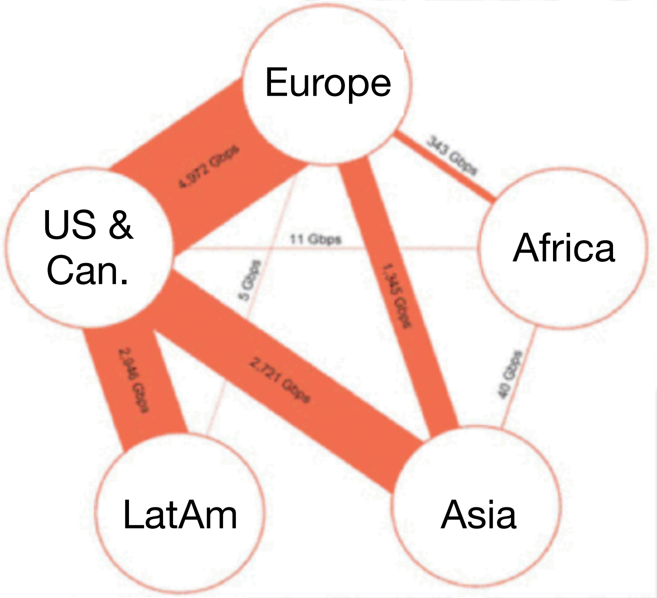


These Apps Are Putting a Strain on Mobile Networks
Breakdown of peak period mobile internet traffic in North Amerika by application

Data gathered in September and October 2015
Source: Sandvine



Traffic patterns in the Wifirst network (French ISP)



Intl Internet Regional Capacity (2011), src: Telegeography Research

- Systems **integration** : pre-existing communication systems (television, telephone) are becoming part of (or dependent on) the Internet
  - As well as critical infrastructures for society (energy grid, transportation systems, healthcare)
  - Exposed to their vulnerabilities too !
- If you are connected, you are exposed : deal with intrusions, anomaly detection, etc.
- "*With great power comes great responsibility*"
  - Not only against malicious agents; also in terms of safety

Take-aways

- Internet was not designed to become the open, critical infrastructure it is today

- Security was not a design concern : devices/participants were assumed to be “trusted parties”
  - (Except, robustness for survivality)

- Fragile in the core (BGP), fragile in the edge (DHCP, DNS, TCP) => based on trust

- Internet is absorbing/integrating pre-existing telecommunication systems (telephone, cellular system, television…)

- Centralization entails vulnerability
  - A few number of entities (operators, service providers, networks) generate/carry/attract an increasing share of Internet traffic

- Wireless communications are inherently insecure (everybody is listening !)

- Emergence of the IoT dramatically increases the scope of cybersecurity risks
  - Pervasiveness of connected objects and systems: ~50 billion connected objects!
  - Aggregate computing resources for cyberattacks: growing concern on DDoS
  - Critical infrastructures (electrical grid, transportation systems, etc.) increasingly depend on it

- Yes, technological advances may put at risk cryptographic mechanisms…
  (Moore’s law, quantum computing)
  - …but the weakest link in the cybersecurity chain is usually non-cryptographic (either user practice or non-cryptographic elements of protocols/mechanisms)

Thanks !

juan-antonio.cordero-fuertes@polytechnique.edu
http://epizeuxis.net

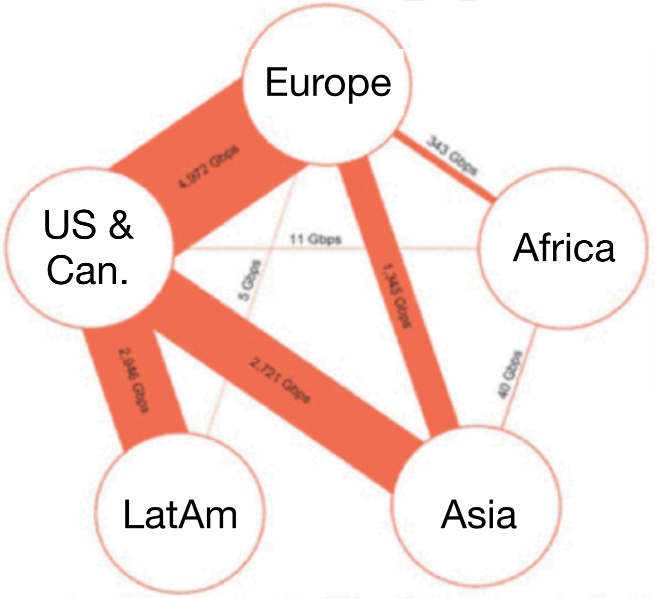
NSA's PRISM and Upstream Collection Programs

- (Exposed by former NSA contractor Edward Snowden in 2013)

- Verizon call-records program: metadata

- **PRISM**
  - NSA program for collection of Internet communications
  - Started in 2007 under the "Protect America Act"
  - US-based Internet service providers (Facebook, Yahoo, Google, Skype, Twitter) required to allow access to user data

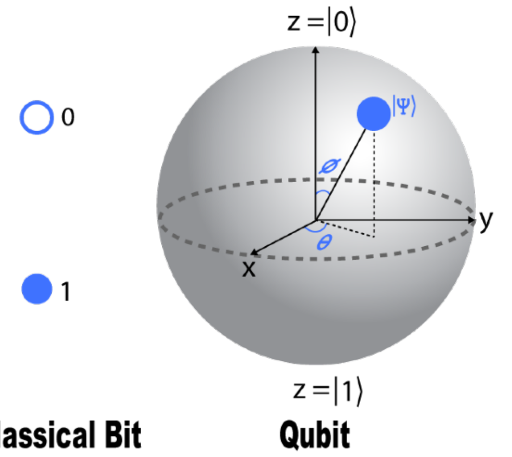
- **Upstream**
  - Set of cable-intercept programs (fiber, other infrastructure), in US soil or abroad
  - A large % of Internet traffic transits through US cables



International Internet Regional Capacity (2011)

Src: Telegeography Research

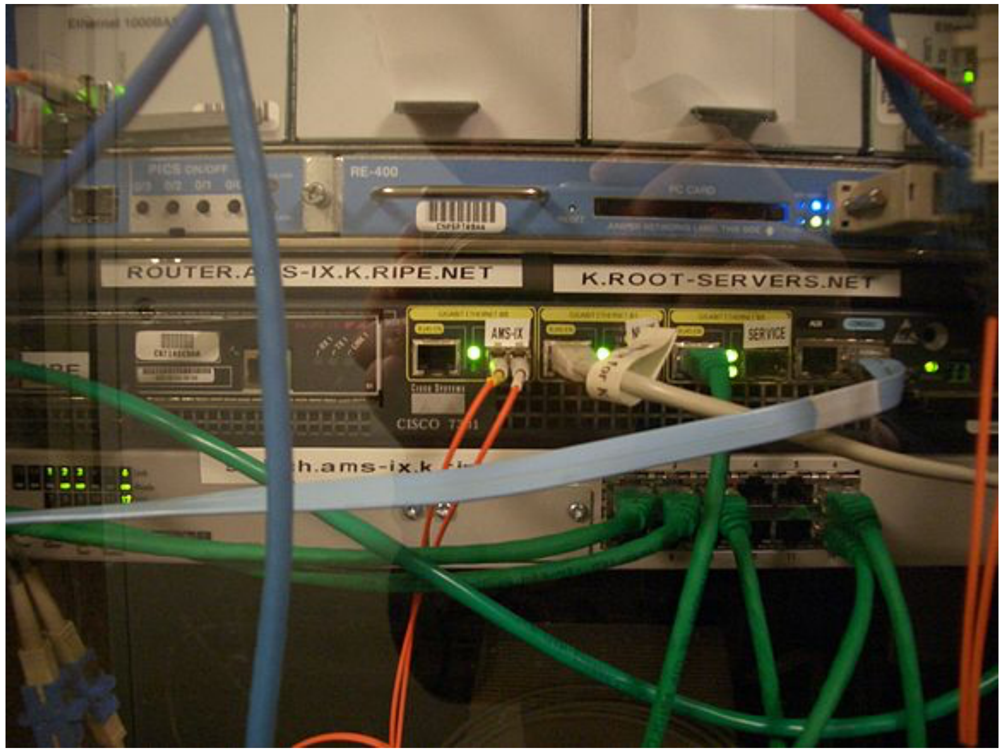
- (source: https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded)



Today's computers, called "classical" computers, store information in binary; each bit is either on or off. Quantum computation use qubits, which, in addition to being possibly on or off, can be both on and off. The unlimited amount of states that a qubit can be in at any given time is traditionally represented in a sphere where North = 1 and South = 0.

When the qubit is represented on a sphere, the angles formed by the radius determine the odds of measuring a 0 or 1.

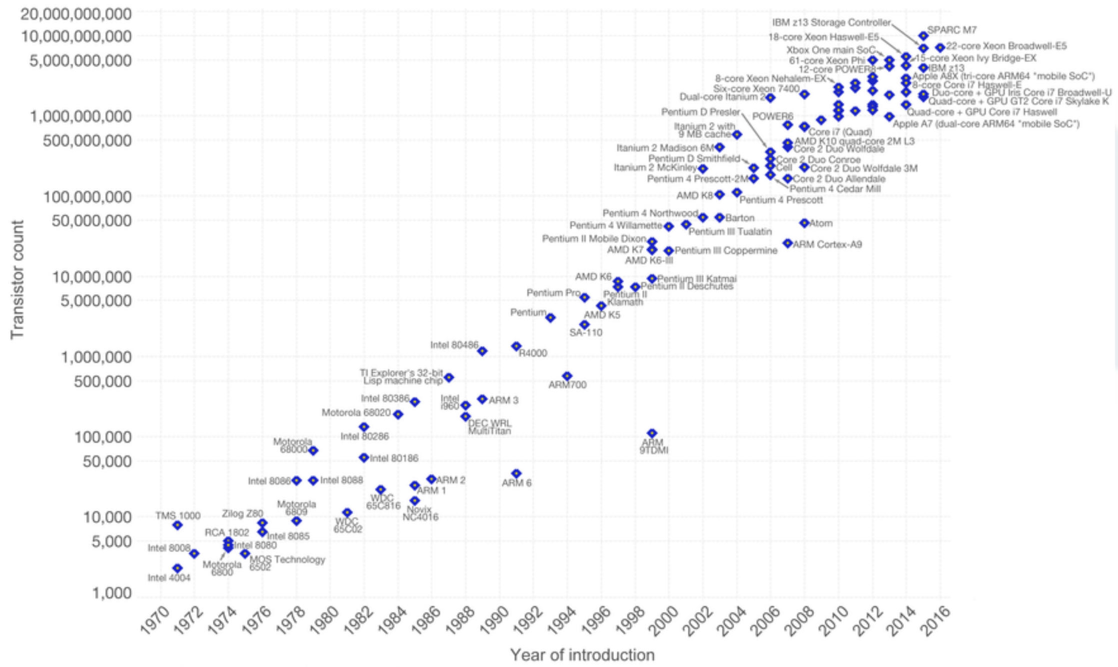
Telefónica data center in Alcalá de Henares, Madrid



A Cisco 7301 router and a Juniper M7i, part of the K root-server instance at AMS-IX

Moore's Law – The number of transistors on integrated circuit chips (1971-2016)

Moore's law describes the empirical regularity that the number of transistors on integrated circuits doubles approximately every two years. This advancement is important as other aspects of technological progress – such as processing speed or the price of electronic products – are strongly linked to Moore's law.

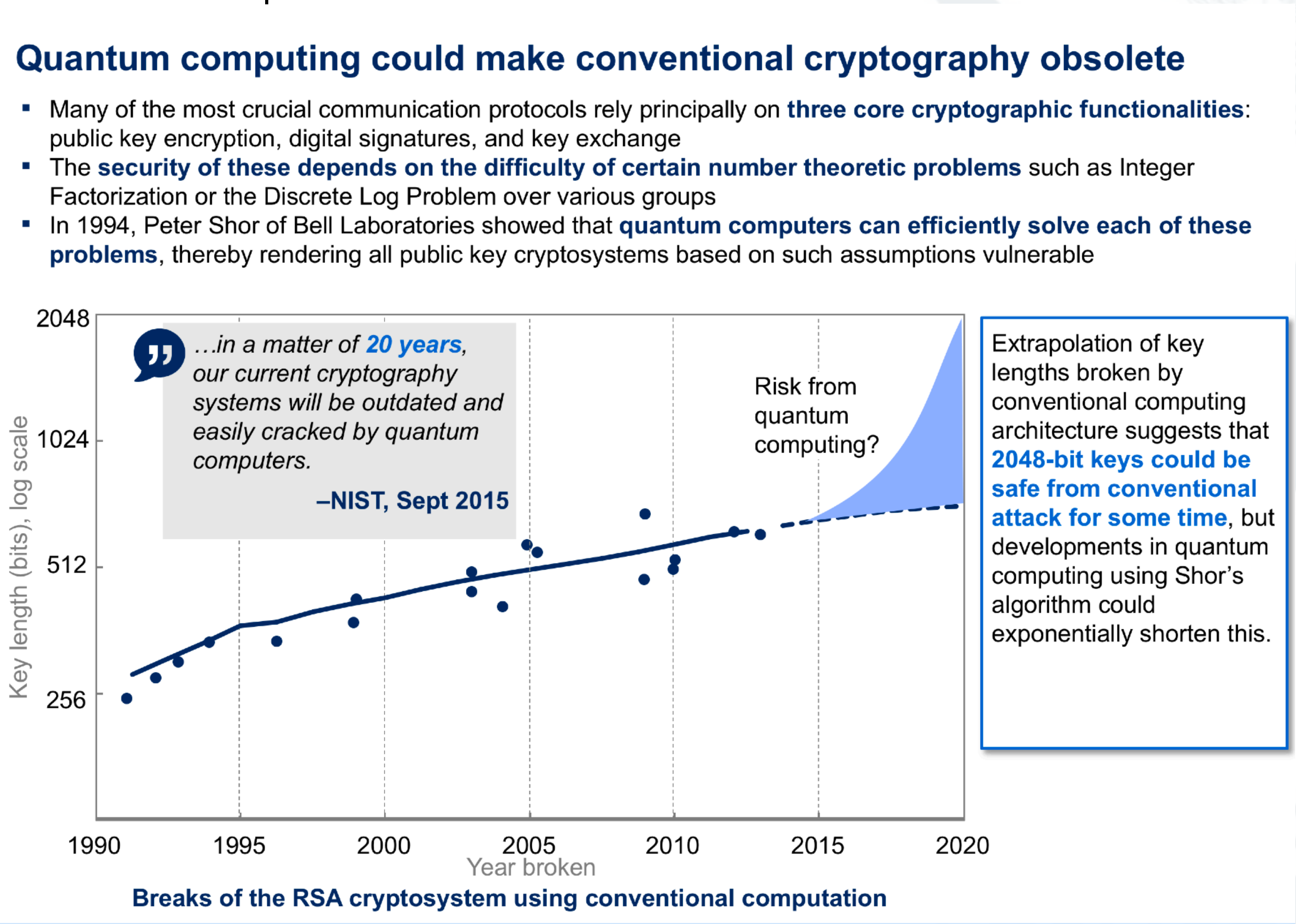


Data source: Wikipedia (https://en.wikipedia.org/wiki/Transistor_count)
The data visualization is available at OurWorldinData.org. There you find more visualizations and research on this topic.

Licensed under CC-BY-SA by the author Max Roser.

Technological advancements

- Quantum Shor’s algorithm could solve factorization problem in polynomial time => RSA compromised



Quantum computing could make conventional cryptography obsolete

- Many of the most crucial communication protocols rely principally on **three core cryptographic functionalities**: public key encryption, digital signatures, and key exchange
- The **security of these depends on the difficulty of certain number theoretic problems** such as Integer Factorization or the Discrete Log Problem over various groups
- In 1994, Peter Shor of Bell Laboratories showed that **quantum computers can efficiently solve each of these problems**, thereby rendering all public key cryptosystems based on such assumptions vulnerable

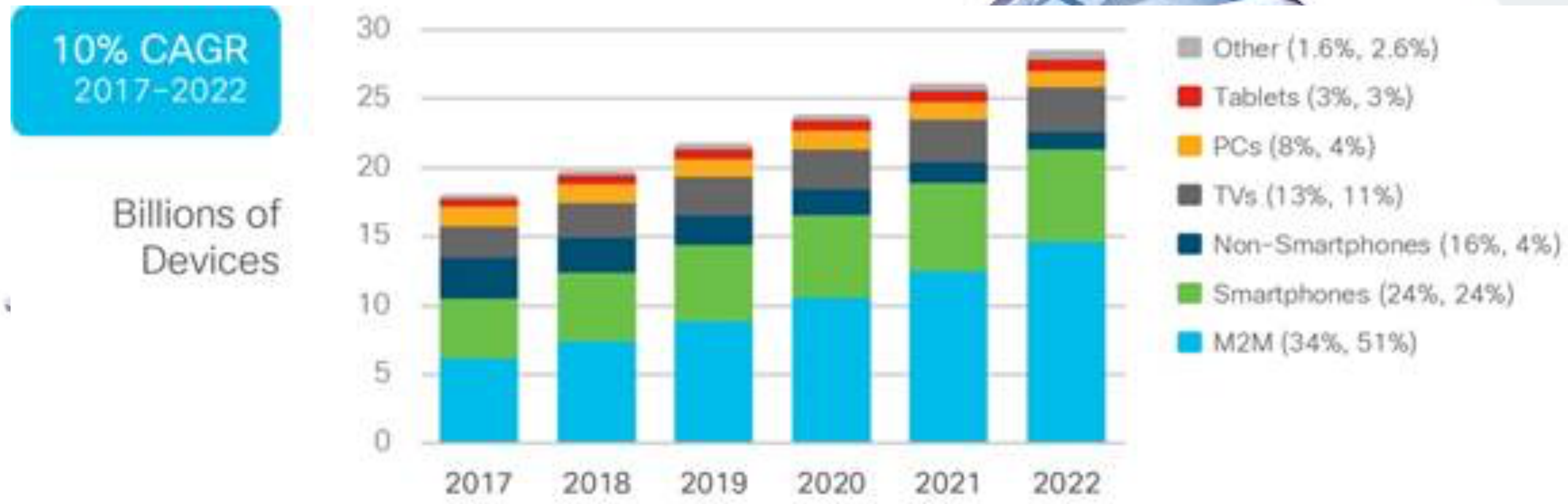
> *…in a matter of **20 years**, our current cryptography systems will be outdated and easily cracked by quantum computers.*
>
> **–NIST, Sept 2015**

Breaks of the RSA cryptosystem using conventional computation

Extrapolation of key lengths broken by conventional computing architecture suggests that **2048-bit keys could be safe from conventional attack for some time**, but developments in quantum computing using Shor’s algorithm could exponentially shorten this.

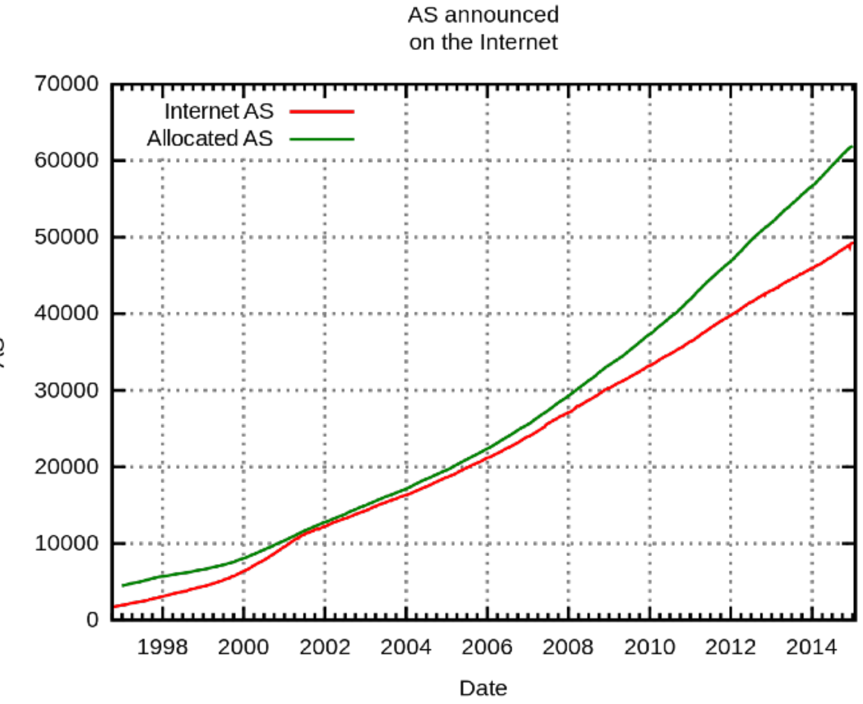
Some (more or less famous) relevant cyberattacks

- 1988: Morris worm, first (unintentional) DDoS attack
  - ~6000 computers affected (10% Internet devices at the time), ~100M USD damage
- 1999: Melissa virus, as attachment via mail, using MS-Office to spread, 80M USD damage
  - Teenager Jonathan James hacks NASA and US DoD networks
- 2000: Mafiaboy's DDoS attack against Amazon, eBay, Yahoo!, ~1200M USD damage
- 2002: 1-hour DDoS attack against the 13 root DNS servers
- 2013: Attacks on Yahoo! : 500M and 1000M user accounts compromised
- 2014: BGP attack, Google DNS 8.8.8.8 hijacked, traffic re-routed to Venezuela and Brazil servers
- 2015, 2016: Attacks on AshleyMadison and AdultFriendFinder : 60 GB of account information and 400M accounts compromised, respectively
  - Poor password protection with SHA-1 hash
- 2016: DDoS attack against DynDNS (affecting GitHub, Twitter, Spotify, Paypal, etc.)
  - Hacked IOT devices, infected by Mirai malware, used as "zombie armies"
  - ~50K IOT devices involved in 164 countries, traffic peaks of 280 Gbps
  - (ref. https://www.incapsula.com/blog/malware-analysis-mirai-ddos-botnet.html)
- 2017, 2018
  - WannaCry ransonware attack (NHS, Telefonica, FedEx, etc.), 4000M USD damage estimated
  - Attacks on Equifax (140M accounts compromised, with users critical data), and security leakage from Exactis (340M accounts exposed)
- Src: https://www.gomindsight.com/blog/history-of-cyber-attacks-2018/, https://www.arnnet.com.au/slideshow/341113/top-10-most-notorious-cyber-attacks-history/, https://thehackernews.com/2014/03/google-public-dns-server-traffic.html



* Figures (n) refer to 2017, 2022 device share

Source: Cisco VNI Global IP Traffic Forecast, 2017-2022


AS announced
on the Internet
Internet AS
Allocated AS
Date