Cyber security – don't be a victim!

Corrado Giustozzi

Brussels, October 4th, 2017

selta.com

Our (short) journey

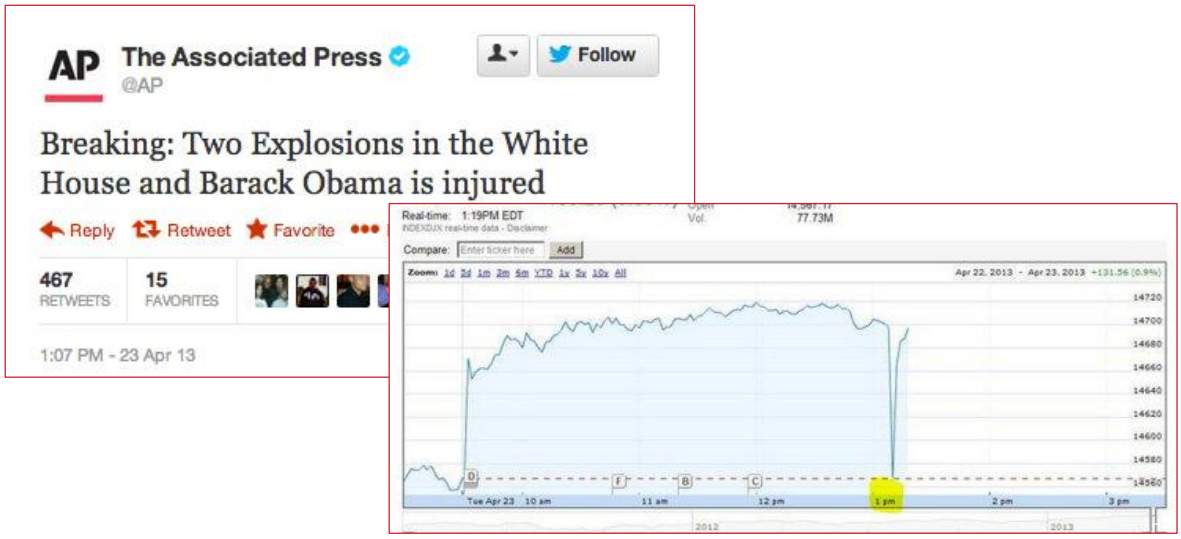
- Preface
- Once upon a time
- What does it mean?
- Conclusion

Preface: the value of information

Information is power

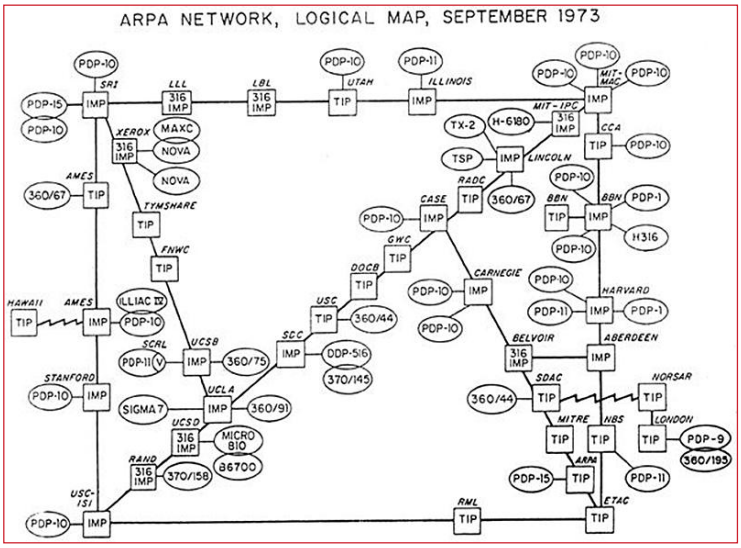
- The world's largest taxi company **owns no vehicles**
  - 62,5 G$ → 15 × Hertz
- The most popular media provider **creates no content**
  - 267 G$ → 130 × NYTimes
- The largest accomodation provider **owns no real estate**
  - 25 G$ → 8 G$ > Hilton (745.000 rooms in 4.500 hotels)
- The most valuable retailer **has no inventory**
  - 268 G$ → 69 G$ > Wall Mart (10.000 stores)

Non-proportional impacts



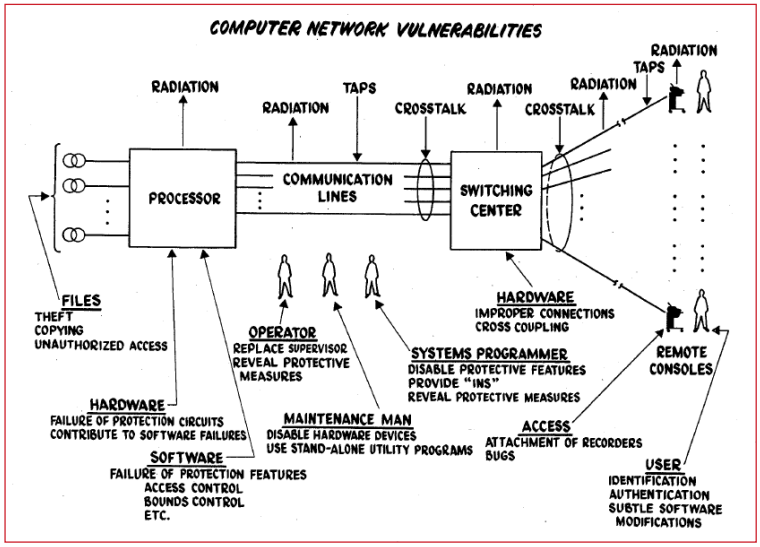
Once upon a time…

ARPAnet in 1973



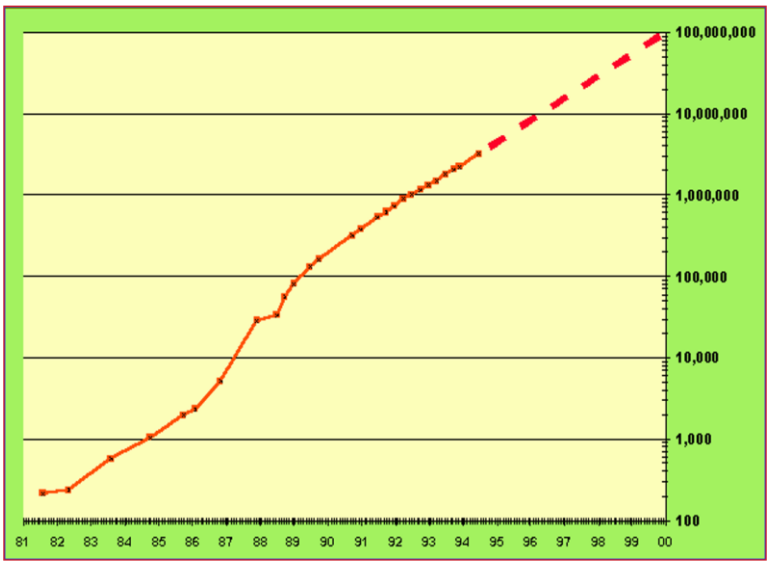
Source: The Internet Society

Computer / network security in the '70s



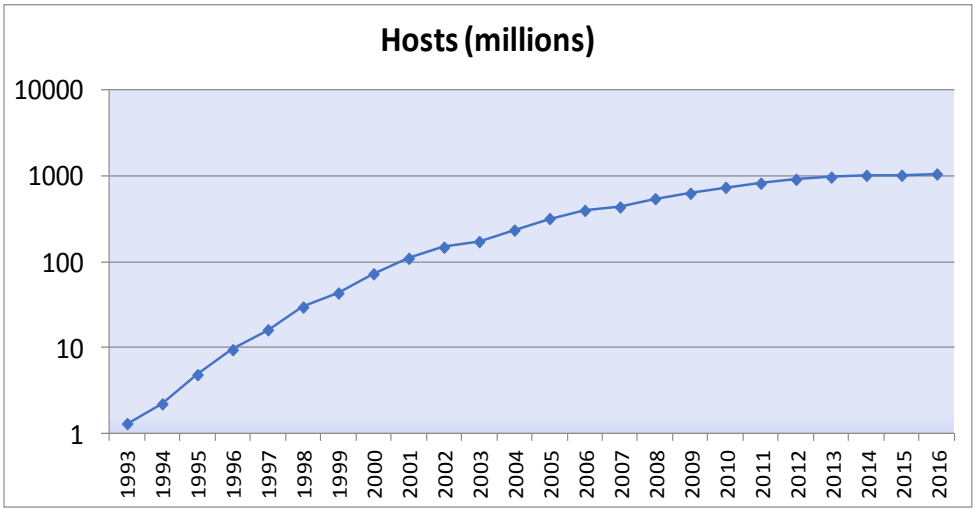
Source: "The Ware report", Rand Corp., 1970

Internet growth, 1981-1994 and beyond



Source: The Internet Society

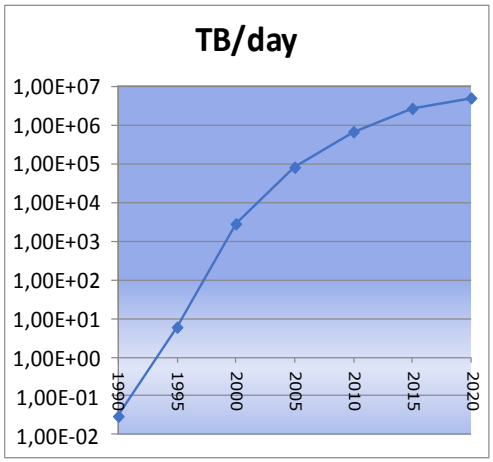
Internet actual growth, 1993-2016



Source: Statista, 2017

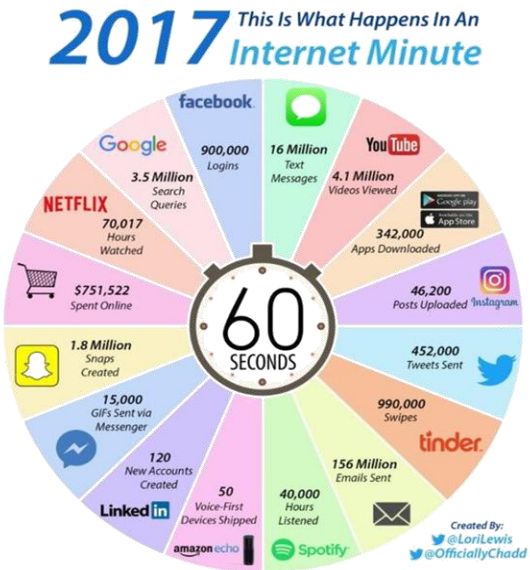
Traffic growth, 1990-2020

Year	TB/day	F_{1990}
1990	0.03	1
1995	6	$2.0 \cdot 10^2$
2000	2,800	$9.3 \cdot 10^4$
2005	81,000	$2.7 \cdot 10^6$
2010	672,000	$2.2 \cdot 10^7$
2015	2,680,000	$8.9 \cdot 10^7$
2020	5,000,000	$1.7 \cdot 10^8$



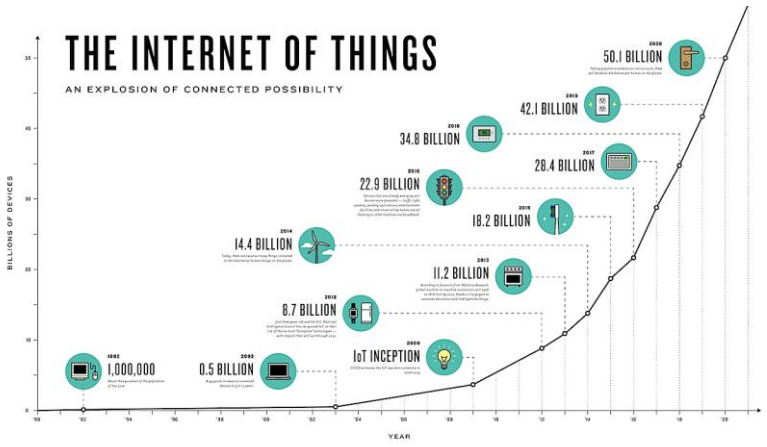
Source: Cisco VNI, 2011, 2015

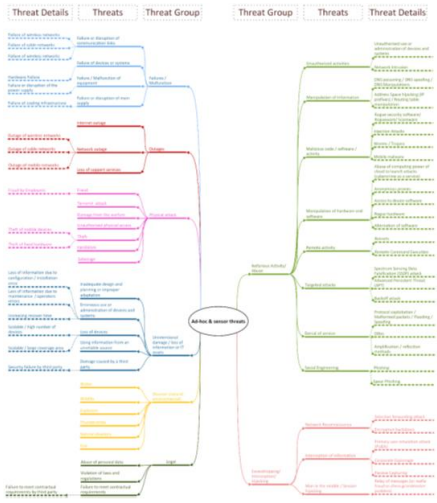
The numbers of the Internet



- **Devices**: in 2019 the number of network connected devices will be more than three-and-a-half that of the Earth population.
- **Traffic**: IP traffic in 2015 was 72,4 HBytes per month. In 2019 it will be 168,0 HBytes per month. *(1 HByte = 10^{18} Bytes, that is one billion GBytes).*
- **Users**: they were 3 billions in 2015, will be 4 billions in 2019.

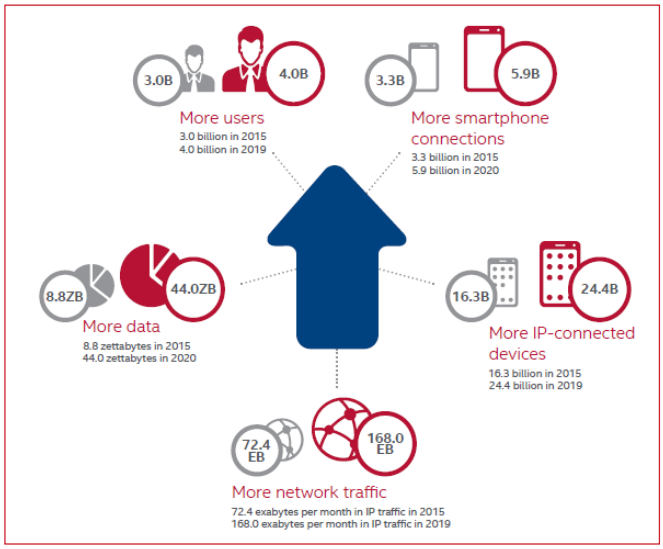
And… hold on, IoT is coming!





What does it mean?

Attack surface is broadening



Souce: McAfee Labs, 2015

Living in a small (and vulnerable) planet

- Cyberspace is not a world apart or a different dimension, but the connected set of all the systems and networks on our planet
  - cyber threats are global and pervasive, not limited to the Cyberspace itself in that they are able to affect real-world infrastructures: the so called **cyber-physical domain**
- Cyberspace is often considered a «no-man-land» because it lacks explicit borders and a clear jurisdiction
  - actually it is a sort of «teleporter» that enables everyone to project its presence and activities right into the heart of another nation's systems without the need to cross any real border: the cyberspace **is not topological**
- The benefit-cost ratio of a cyber attack is getting higher and higher because it is easier and easier to reach the critical infrastructures and exploit the inherent weaknesses affecting many of them

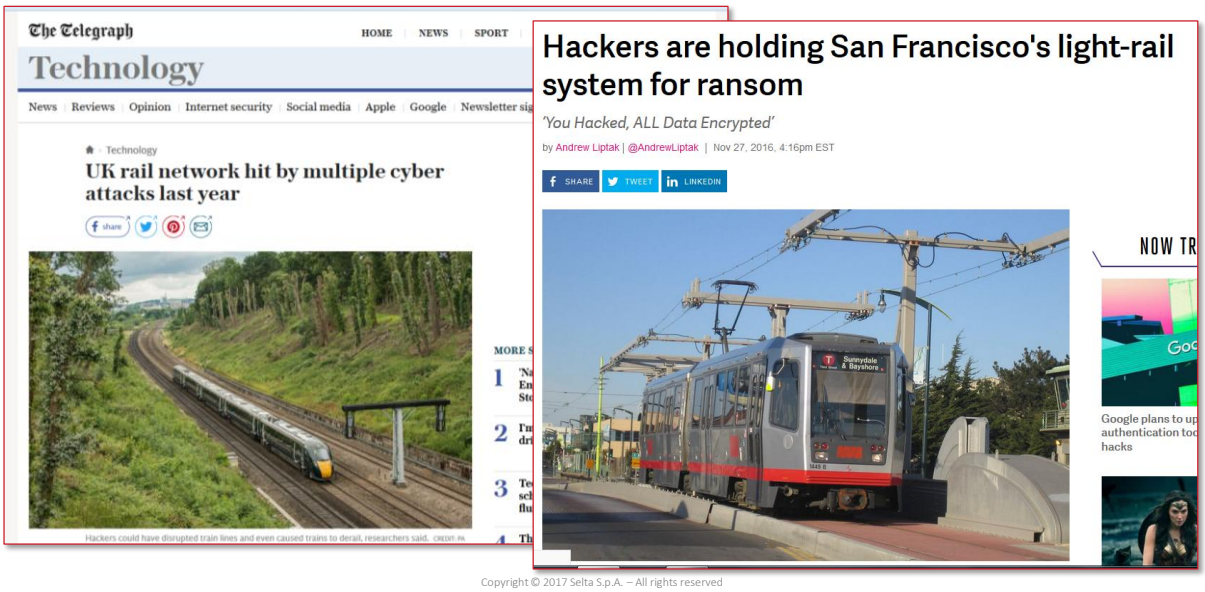
Do we really need security?...

- In the good ol' days we didn't need security
  - …or, did we?
- The first Internet was designed with no security in mind
  - everyone was supposed to act in good faith
- The same happened with many later technologies, which didn't take into account threats from fraudsters, criminals, terrorists, …
- Assumption was: "we don't need security because…":
  - …we are not doing anything secret/valuable
  - …we don't have enemies/adversaries
  - …physical security is enough (no or difficult remote access)
  - …the system is so complex/obscure that no one can possibly tamper with it (because of the lack of money/time/knowledge/technology…)

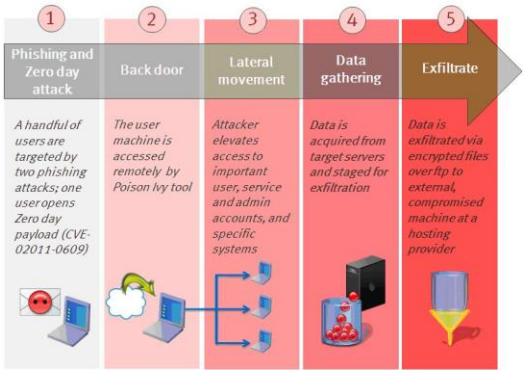
An easy game for the bad guys

- Cyber adversaries exploit relevant weaknesses in their targets
- Technical weaknesses:
  - insecurity by design (weak/no authentication, no cryptography, …)
  - protocols are often flawed and/or bugged
  - systems are bugged and/or not enough protected
- Complexity weaknesses:
  - systems/networks complexity is overwhelming
  - there are simply too many people/devices on the Net
  - traffic volume is becoming unmanageable
- Human/behavioural weaknesses:
  - no awareness and/or security culture by the end users
  - fundamental assumption is good faith on everyone else's part

That leads to either direct attacks…



…and sophisticated triangulations



LOCKHEED MARTIN

What we can do

The only way to cope: cooperation

- The best (only?) way to cope with the increasing threats is **cooperation**
- The NIS Directive represents the first EU-wide rules on cybersecurity
- Its objective is to achieve a **high common level of security** of network and information systems within the EU, by means of:
  - improved cybersecurity capabilities at national level
  - increased cooperation at EU level
  - risk management and incident reporting obligations for operators of essential services and digital service providers
- To increase cooperation at EU level, the NIS Directive establishes:
  - a Cooperation Group, to support and facilitate strategic cooperation and the exchange of information among Member States
  - a network of the national CSIRTs, to contribute to the development of confidence and trust between the Member States and to promote effective operational cooperation

In the cyberspace none of us is an island

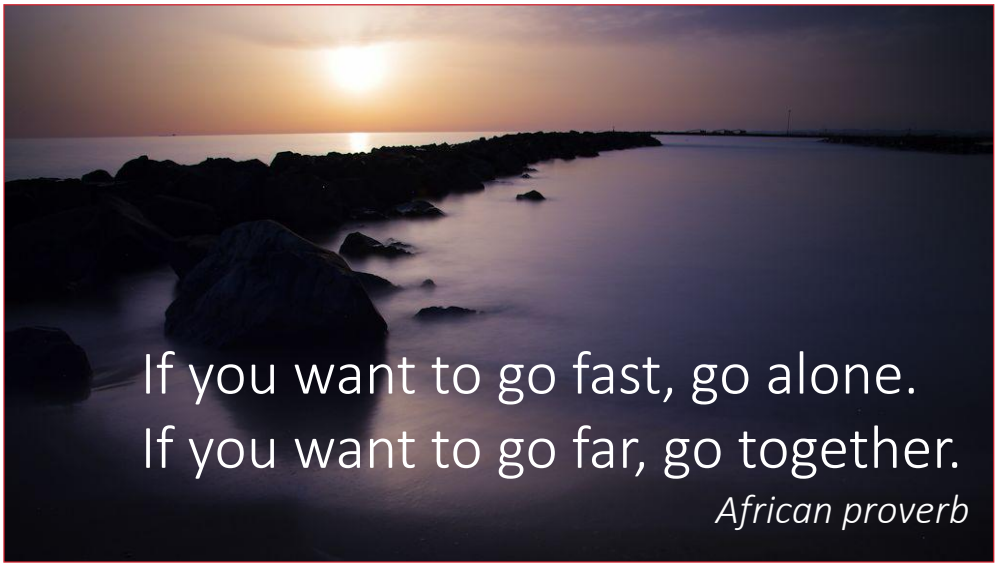


Image © 2013 Corrao Giustozzi

Linking The Future

conference 2017 CyberSecurity4Rail

Thank you for your attention

corrado.giustozzi@selta.com

@cgiustozzi

selta.com