UNIVERSITÀ DEGLI STUDI FIRENZE

The Cybersecurity in the European Union

The NIS Directive

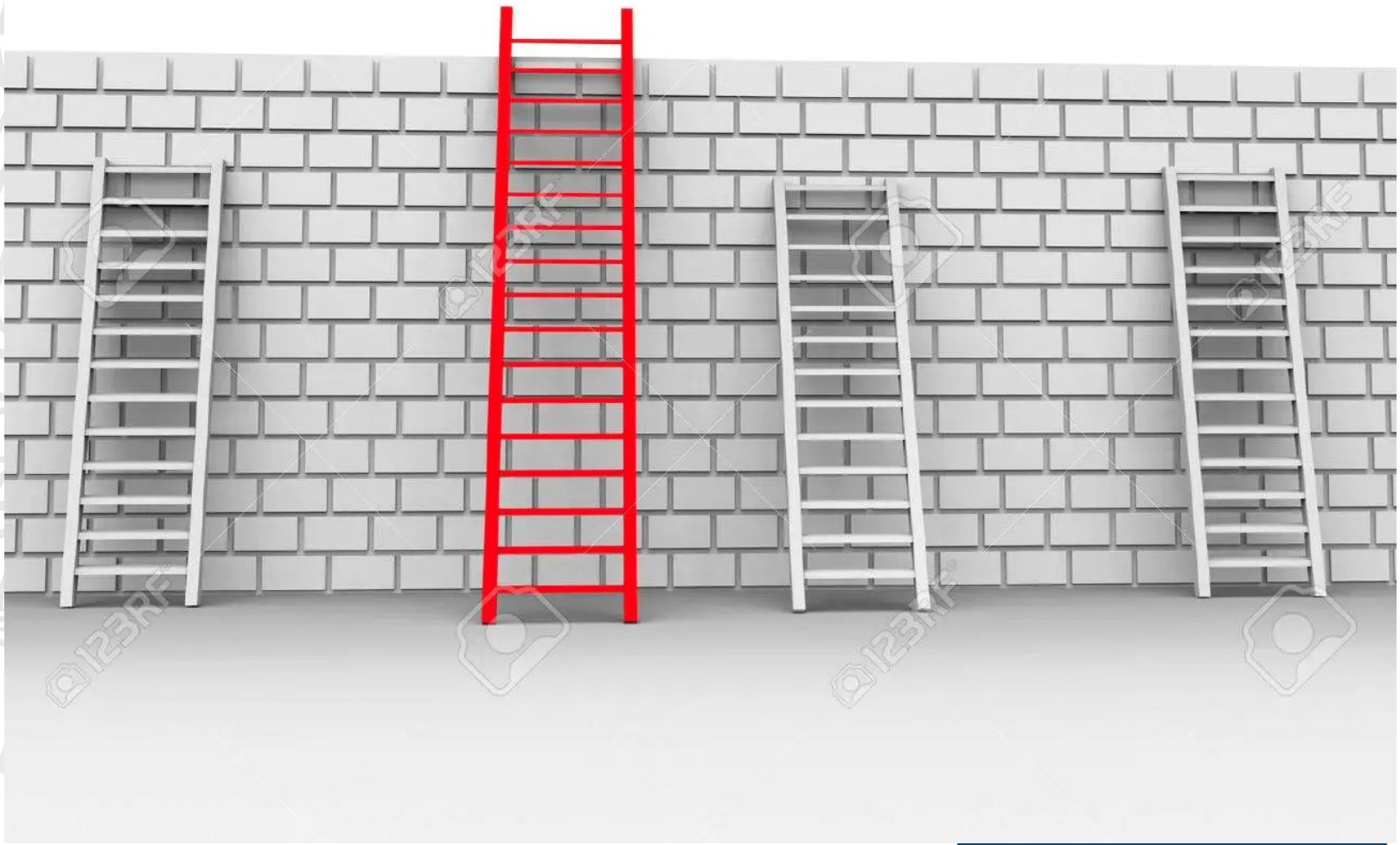
Erik Longo - Matteo Giannelli

Iniziativa organizzata all'interno del progetto

ARC GDPR AWARENESS RAISING CAMPAIGN FOR SMEs

Torino 6 febbraio 2024

LAW



The evolution of cybersecurity

- *Computer security*
- *Information security*
- *(digital) life security*

The Evolution of Cybersecurity

Cybersecurity is no longer a technological 'option', but a societal need and a value. Examples:

- Critical infrastructures
- Magnitude of the impact
- Complexity and duration of attacks
- Computational power
- Societal aspects
- Great opportunities
- New dangers (e.g. COVID; war)

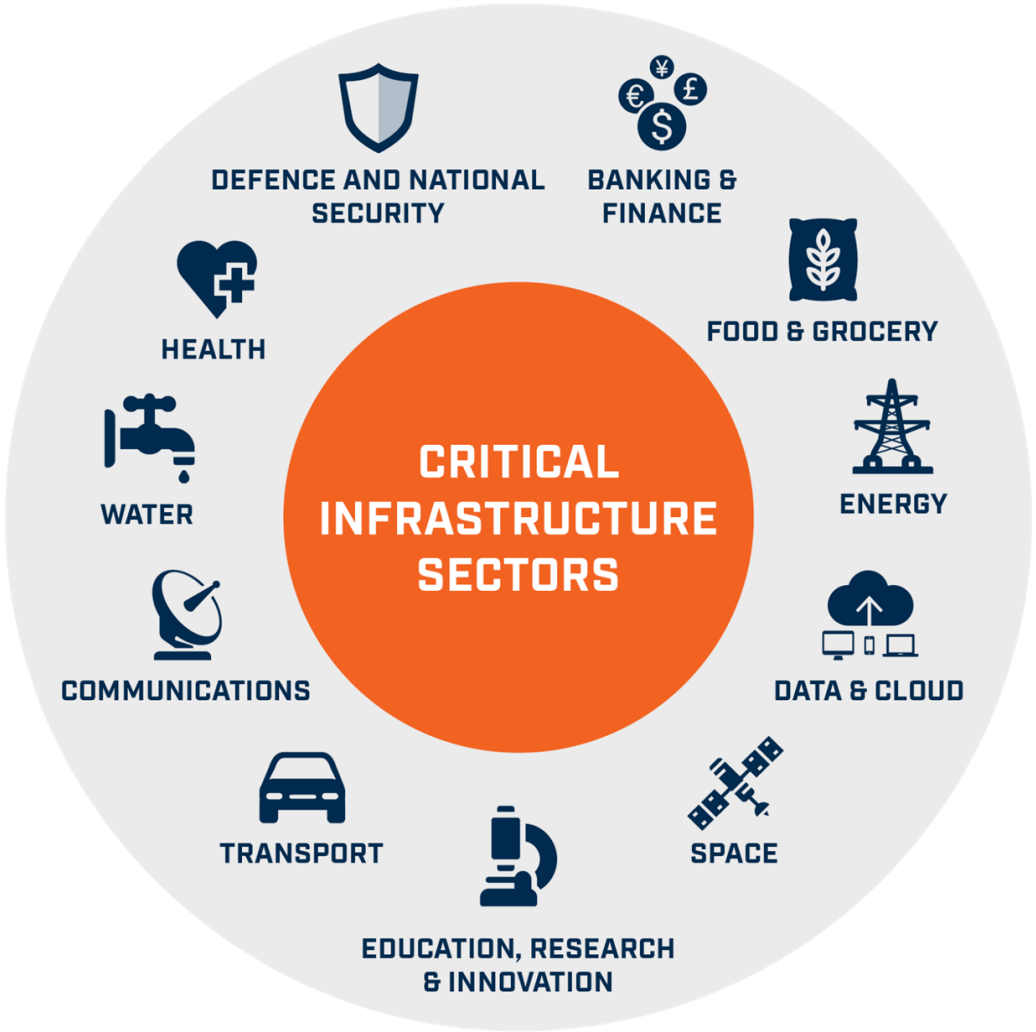
How to build a European society secure by design?

The Evolution of Cybersecurity

Cybersecurity is no longer a technological 'option', but a societal need and a value. Examples:

- **Critical infrastructures**
- Magnitude of the impact
- Complexity and duration of attacks
- Computational power
- Societal aspects
- Great opportunities
- New dangers (e.g. COVID; war)

How to build a European society secure by design?

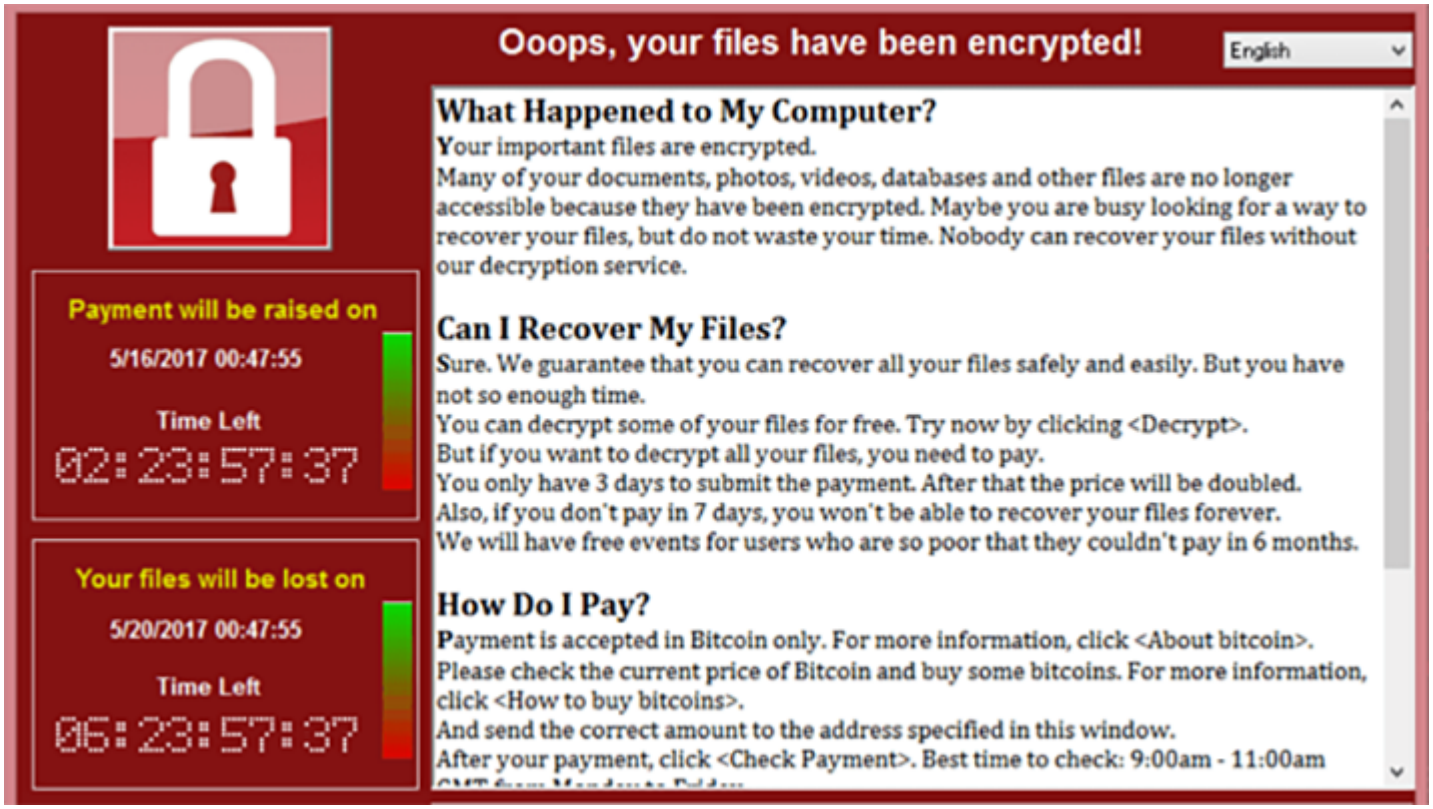

DEFENCE AND NATIONAL SECURITY
BANKING & FINANCE
HEALTH
FOOD & GROCERY
WATER
ENERGY
CRITICAL INFRASTRUCTURE SECTORS
COMMUNICATIONS
DATA & CLOUD
TRANSPORT
SPACE
EDUCATION, RESEARCH & INNOVATION

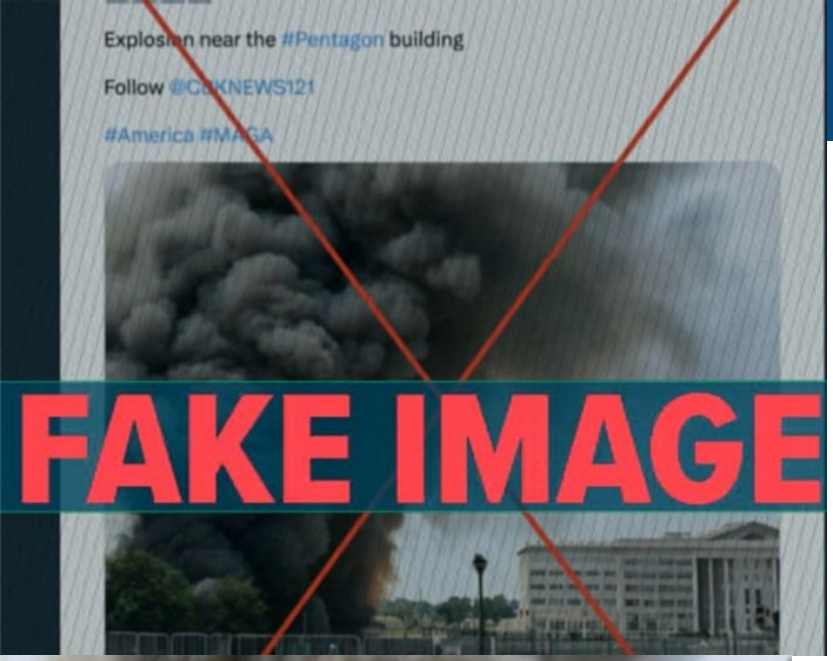
The Evolution of Cybersecurity

Cybersecurity is no longer a technological 'option', but a societal need and a value. Examples:

- Critical infrastructures
- **Magnitude of the impact**
- Complexity and duration of attacks
- Computational power
- Societal aspects
- Great opportunities
- New dangers (e.g. COVID; war)

How to build a European society secure by design?


Ooops, your files have been encrypted!
English
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.
How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am
Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37
Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37


Explosion near the #Pentagon building
Follow @C
KNEWS121
#America #MAGA
FAKE IMAGE


US500
M5
4222.3
4219.8
4217.2
4214.7
4212.1
4209.6
4207.0
4204.5
4201.4
4199.4
4196.8
4194.3
4191.7
4189.2
4186.6
4184.1
4181.5
SMA [200, 0] 4202.5
SMA [50, 0] 4205.7
01m 49s
22.05.2023 08:35
09:25
10:15
11:05
11:55
12:45
13:35
14:25
15:15
16:05


AI-generated image

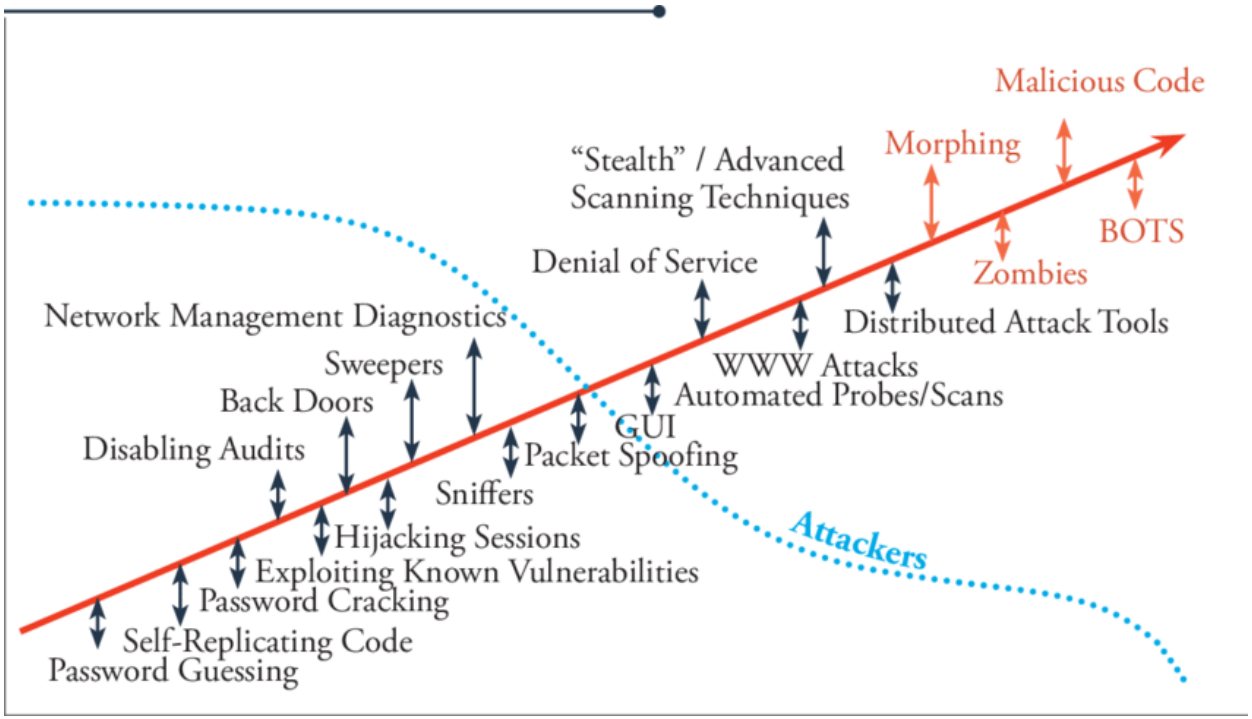

New York
9:15 AM
AI-GENERATED FAKE IMAGE
DIGITAL DANGER
VERIFIED TWITTER ACCOUNTS SHARE FAKE IMAGE OF PENTAGON "EXPLOSION"
Building shown does not closely resemble the Pentagon
CNN
FIRST MOVE

The Evolution of Cybersecurity

Cybersecurity is no longer a technological 'option', but a societal need and a value. Examples:

- Critical infrastructures
- Magnitude of the impact
- **Complexity and duration of attacks**
- Computational power
- Societal aspects
- Great opportunities
- New dangers (e.g. COVID; war)

How to build a European society secure by design?


Malicious Code
Morphing
"Stealth" / Advanced
Scanning Techniques
BOTS
Zombies
Denial of Service
Distributed Attack Tools
Network Management Diagnostics
WWW Attacks
Sweepers
Automated Probes/Scans
Back Doors
GUI
Disabling Audits
Packet Spoofing
Sniffers
Attackers
Hijacking Sessions
Exploiting Known Vulnerabilities
Password Cracking
Self-Replicating Code
Password Guessing

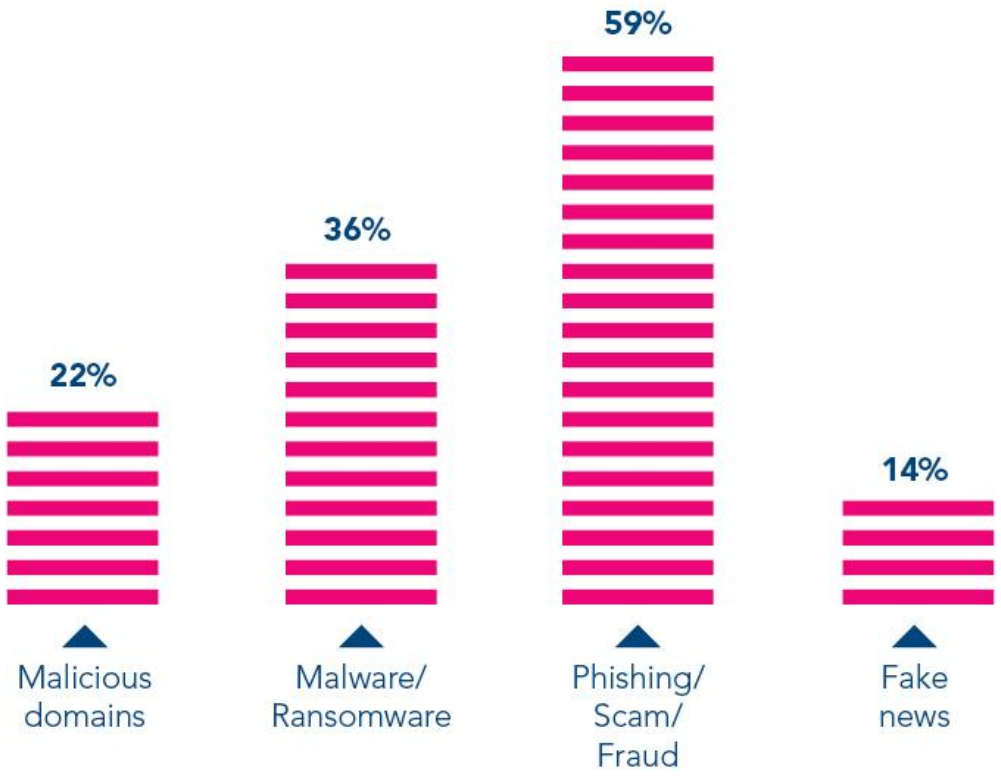
The Evolution of Cybersecurity

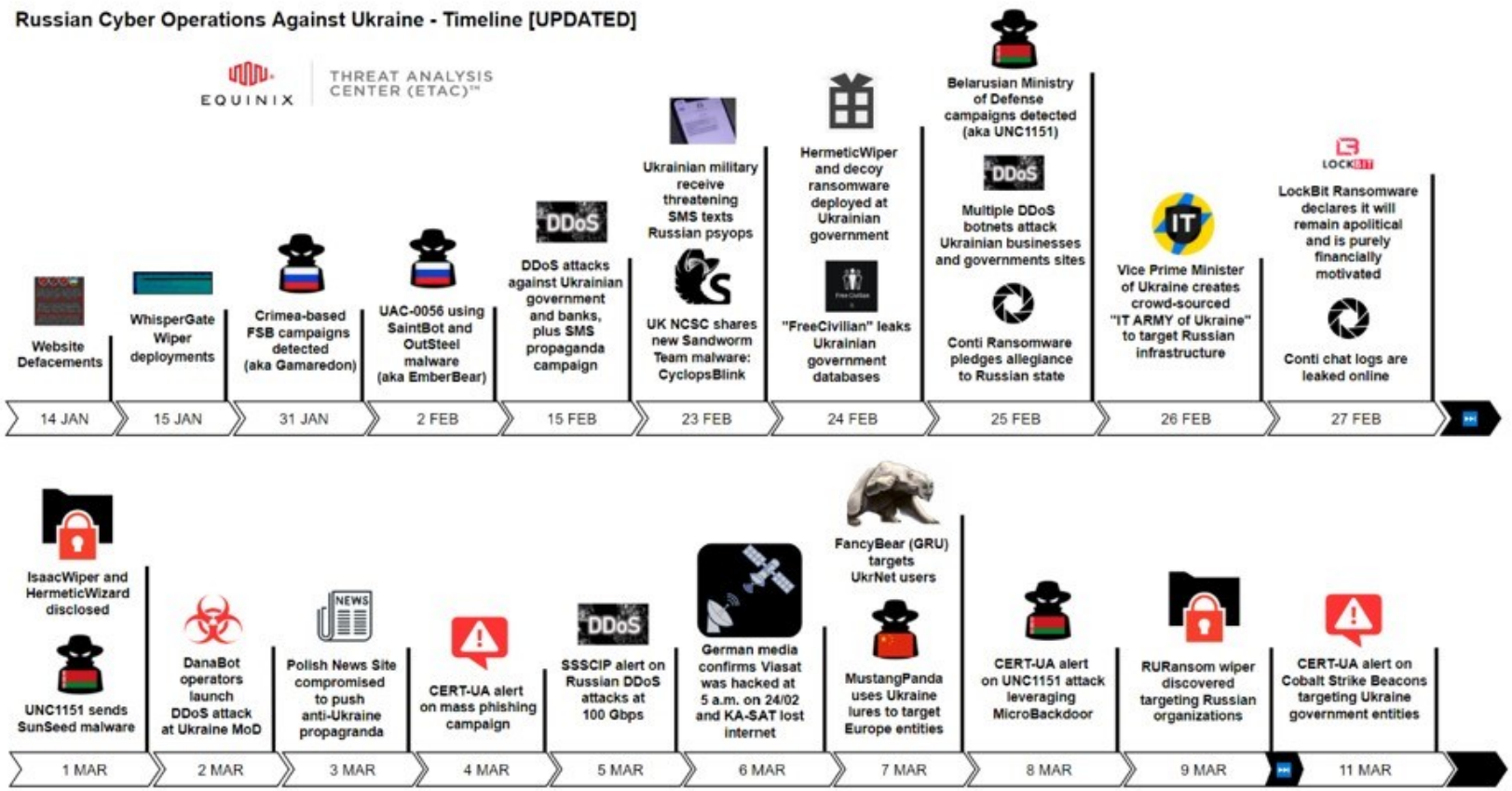
Cybersecurity is no longer a technological 'option', but a societal need and a value. Examples:

- Critical infrastructures
- Magnitude of the impact
- Complexity and duration of attacks
- Computational power
- Societal and economic aspects
- Great opportunities
- **New dangers** (e.g. COVID; war)

How to build a European society secure by design?

Distribution of the key COVID-19 inflicted cyberthreats based on member countries' feedback





Source: https://github.com/curated-intel/Ukraine-Cyber-Operations

The cybersecurity challenge ahead

Three trends in the last 40 years:

1. The circular sequence of **new technology**; new cybersecurity **threats** and **vulnerabilities**; new **mitigations**.
2. The constant increase over the years of the potential **magnitude of attacks** in term of size of targets and impact.
3. A general increase in the **attack surface**.

…yet cybersecurity is costly and crucial

- The number of citizens impacted simultaneously by a single cyber incident can be huge as a **consequence** of the **pervasiveness** of connected devices.
- Cyber attacks are also becoming more and more complex, demonstrating the attackers' enhanced planning **capabilities** and **knowledge**.
- As cyber attackers operate **outside** the norms of **regulation** and **law**, this flexibility gives them a significant advantage over defenders who normally do not enjoy such freedom.
- Cybersecurity has an impact on society and is influenced by the attitude of individuals while they are '**living their digital life**'.

A crucial question

Investments are needed to strengthen security, but is it today possible to determine univocally the level of cybersecurity that our society should achieve?

Cybersecurity is not only and investment but a **multipolar relationship** among individuals, corporations, state and local authorities.

A crucial question: why law must consider cybersecurity?

Cybersecurity Today

- Cybersecurity has become a **horizontal multidomain discipline** encompassing many fields and approaches.
- At the European level, cybersecurity is defined in Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 as "the activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats".
- ISO/IEC 27032:2012: Cybersecurity is defined as the "preservation of confidentiality, integrity and availability of information in the cyberspace".

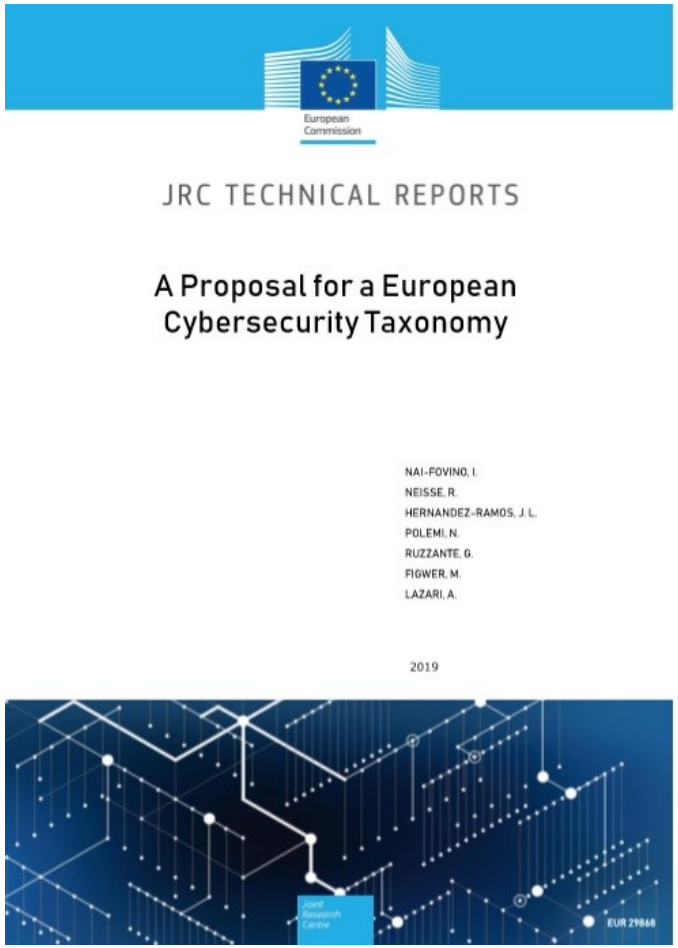
Confidentiality - Integrity - Availability

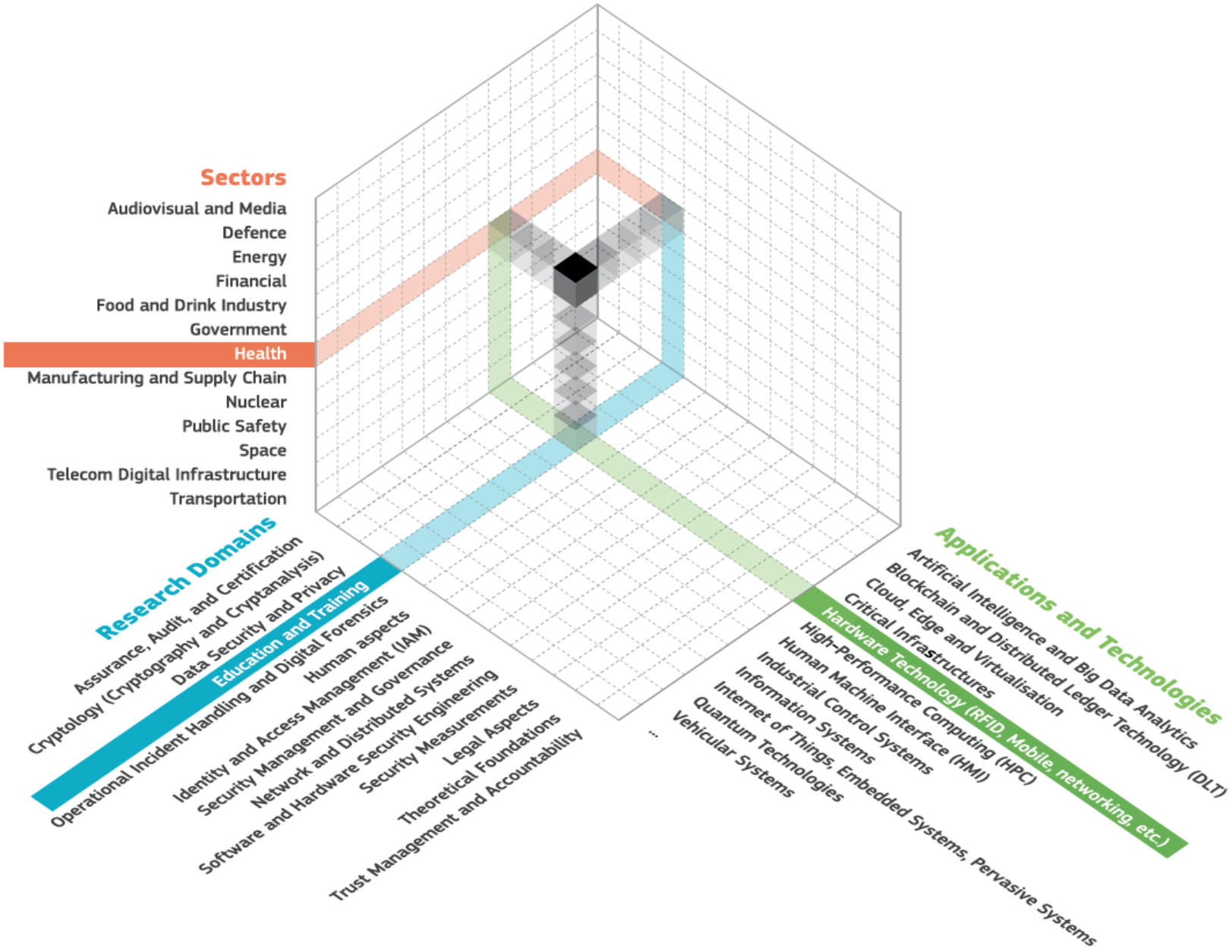
- **Confidentiality** is the concealment of information or resources.
- **Integrity** refers to the trustworthiness of data or resources (and is intended as a set of mechanisms to prevent unauthorised or improper changes).
- **Availability** refers in general to the ability to legitimately use the information or resources (services) desired.

Confidentiality - Integrity - Availability

This taxonomy offers a clear and precise indication of the **areas of fundamental research** and the relevant sectoral domains.

Cybersecurity is shown as a large, multifaceted discipline rather than a sub-area of computer science.




Sectors
Audiovisual and Media
Defence
Energy
Financial
Food and Drink Industry
Government
Health
Manufacturing and Supply Chain
Nuclear
Public Safety
Space
Telecom Digital Infrastructure
Transportation
Research Domains
Cryptology (Cryptography and Cryptanalysis)
Assurance, Audit, and Certification
Data Security and Privacy
Education and Training
Operational Incident Handling and Digital Forensics
Human aspects
Identity and Access Management (IAM)
Security Management and Governance
Network and Distributed Systems
Software and Hardware Security Engineering
Security Measurements
Legal Aspects
Theoretical Foundations
Trust Management and Accountability
Applications and Technologies
Artificial Intelligence and Big Data Analytics
Blockchain and Distributed Ledger Technology (DLT)
Cloud, Edge and Virtualisation
Critical Infrastructures
High-Performance Computing (HPC)
Hardware Technology (RFID, Mobile, networking, etc.)
Human Machine Interface (HMI)
Industrial Control Systems
Information Systems
Internet of Things, Embedded Systems, Pervasive Systems
Quantum Technologies
Vehicular Systems
...

Main takeaways

- Creating **forms of protection** for those who move in cyberspace.
- The frontiers of cybersecurity are **constantly expanding**.
- The security of digital life is a **value for everyone**.

Cybersecurity at the hearth of societal and constitutional transformation

- *In a new world where physical and digital blend together, are the traditional measures to guarantee **trust** sufficient?*
- Cybersecurity is a **need** and a **value** in which privacy, trust and data protection must converge for the building of trust.
- For the technical evolution of digitalization cybersecurity is a necessity.
- The traditional institutions and measures to guarantee trust are no longer sufficient → cybersecurity become our 'digital anchor'.

Cybersecurity and Privacy

- According to the **Article 7** of the CFREU European citizens have the *fundamental right to respect for their private life, home and communications*.
- New privacy threats from digital evolution → there is an urgent need to rethink the way in which online services are designed, putting privacy and cybersecurity at the core of the design process from the outset.
- Improving the level of transparency and usability of online services would facilitate this process → cybersecurity is also a matter of awareness-raising and information.
- There is an abundance of anonymisation tools available → they become powerful tools for attacks.

Cybersecurity and Data Protection

- In the EU data protection is enshrined in the Article 8 of the TFEU and in the GDPR (secondary legislation).
- Experience shows that cybersecurity incidents due to the lack or ineffective implementation of proper data protection and cybersecurity mechanisms can lead to massive personal data breaches.
- Data protection *by design* and *by default* are in line with the principles of security *by design* and *by default* principles well established and adopted by the cybersecurity community.

Cybersecurity and Trust

Businesses, governments and citizens are becoming increasingly concerned by the potential impacts of cyber threats, such as massive personal data breaches, ransomware attacks, cyber extortion campaigns, cyber espionage or state-sponsored cyber attacks.

Ensuring that digital services work safely and securely, while guaranteeing citizens' privacy and data protection, illustrates that cybersecurity has evolved **from a technological 'option' to a societal need**.

The EU Landscape (top-down)

2024 Cyber Resilience Act

2022 NIS 2 Directive

2020 Communication on Shaping Europe's digital future

2020 White Paper on Artificial Intelligence

2020 European Strategy for Data

2019 'Cybersecurity Act'

2017 Joint Communication on Cybersecurity

2016 NIS 1 Directive

2016 GDPR

2013 EU Cybersecurity Strategy

2004 ENISA Reg

What Law Can Do for Cybersecurity

In general there is the need for:

- open debate and eventual decisions on **how to implement** the law in this field.
- clarity, guidelines, concrete legal frameworks and best practices that will ensure both adherence to the law and ethically acceptable behaviour when practising cybersecurity.

Some problems are connected to essentially unsolved larger problems concerning the globalised digital era.

- How to implement cybersecurity measures **combating hate speech or fake information campaigns** without infringing on a citizen's right to freedom of expression?
- How to handle **grey zones** in the usage and dissemination of technology and information that can potentially be misused?
- How can **vulnerability disclosure policies** optimally balance the needs of all stakeholders?
- How to adapt practices in cybersecurity so that they comply with **changing laws**?