Seminario CC5G

La sicurezza informatica nella disciplina recente dell’UE: dalla NIS alla NIS2

Centro di Competenze 5G

Erik Longo - Matteo Giannelli
Università degli Studi di Firenze
Dipartimento di Scienze Giuridiche

POR CreO 2014 2020 Fondo Europeo di Sviluppo Regionale Regione Toscana · FSC Fondo per lo Sviluppo e la Coesione · FUB Fondazione Ugo Bordoni Ricerca e Innovazione · SviluppoToscana S.p.A. · Unione Europea · Repubblica Italiana · Regione Toscana

UNIVERSITA
DEGLI STUDI
FIRENZE

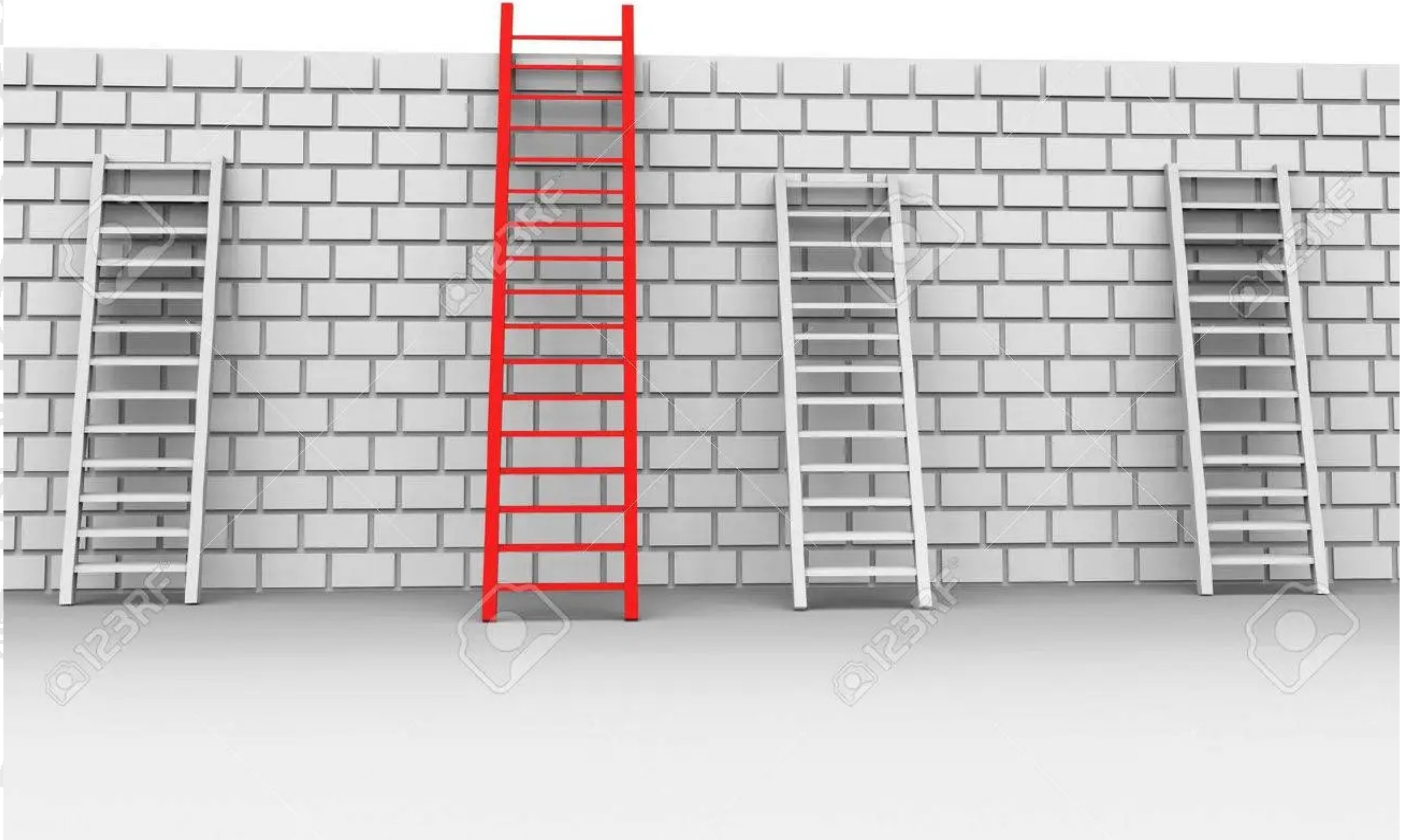
The Cybersecurity in the European Union

The NIS Directive

Erik Longo - Matteo Giannelli

Prato 30 May 2023

LAW



Summary:

Part I

Law and Cybersecurity

Part II

The NIS Directive

Part III

Security obligations in other EU legislation

Part I
Law and Cybersecurity

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)

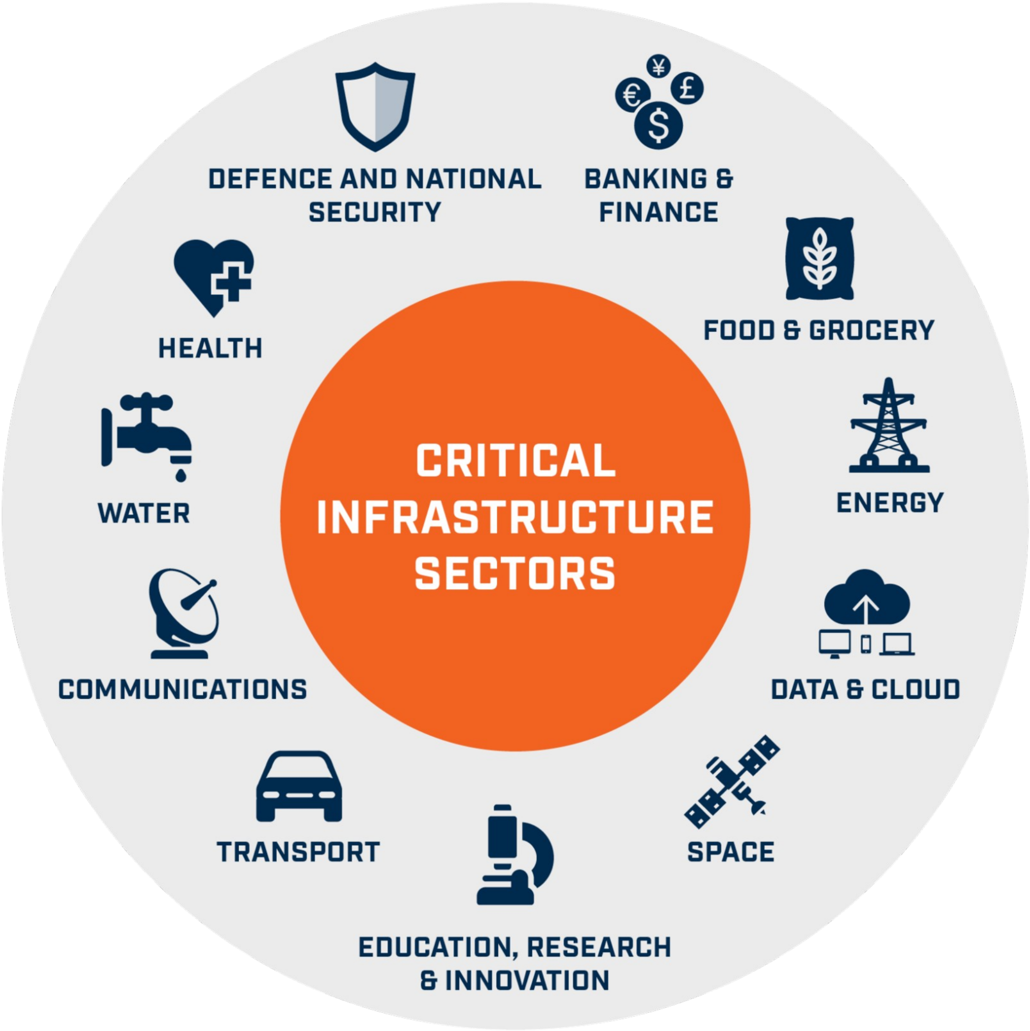
How to build a European society secure by design?

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?

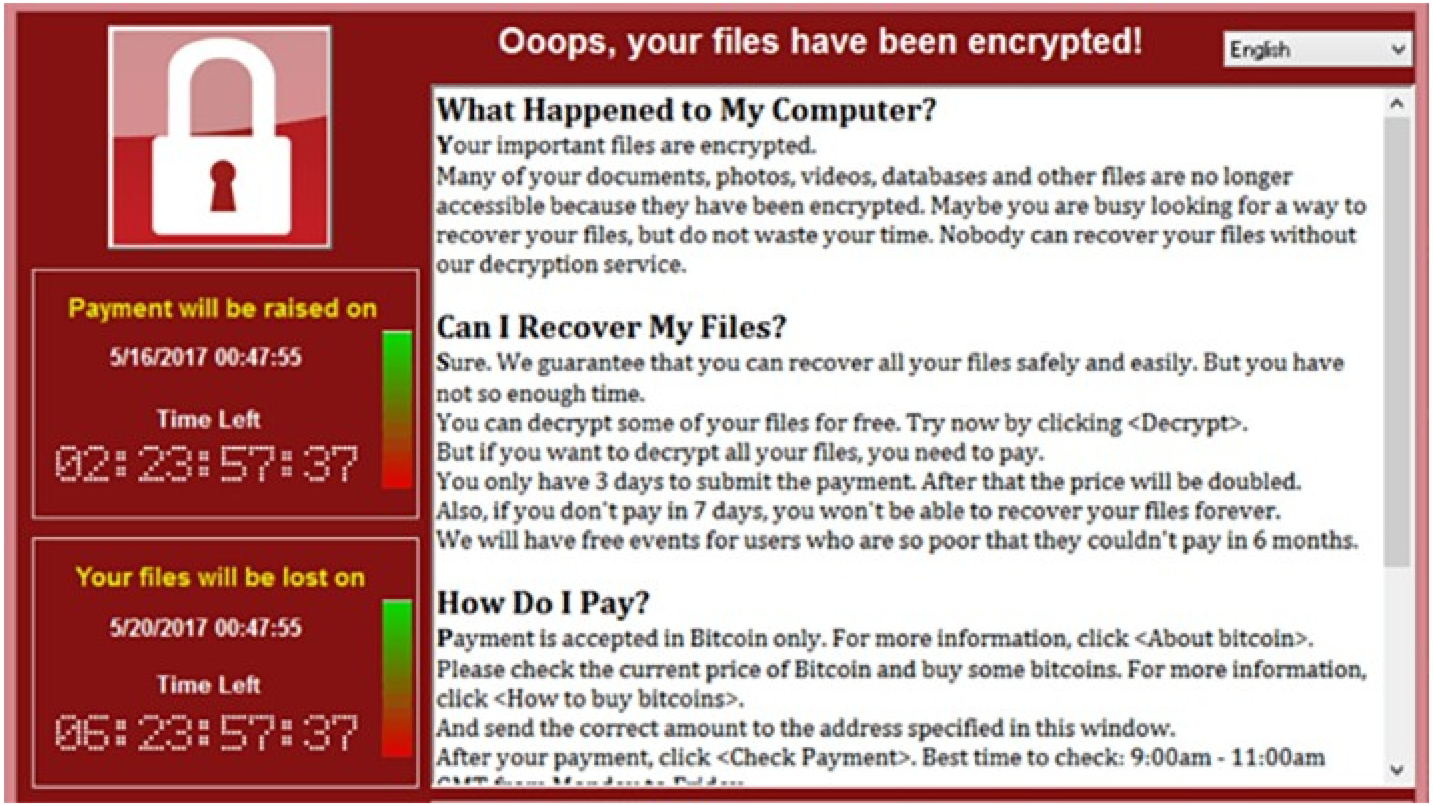

CRITICAL INFRASTRUCTURE SECTORS
DEFENCE AND NATIONAL SECURITY
BANKING & FINANCE
FOOD & GROCERY
ENERGY
DATA & CLOUD
SPACE
EDUCATION, RESEARCH & INNOVATION
TRANSPORT
COMMUNICATIONS
WATER
HEALTH

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!

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

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.

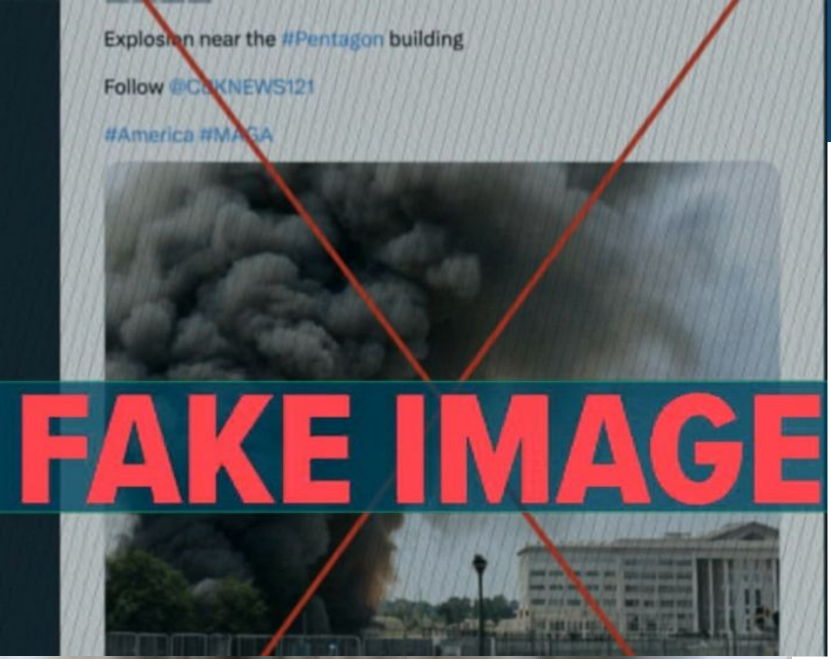
How Do I Pay?

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>.

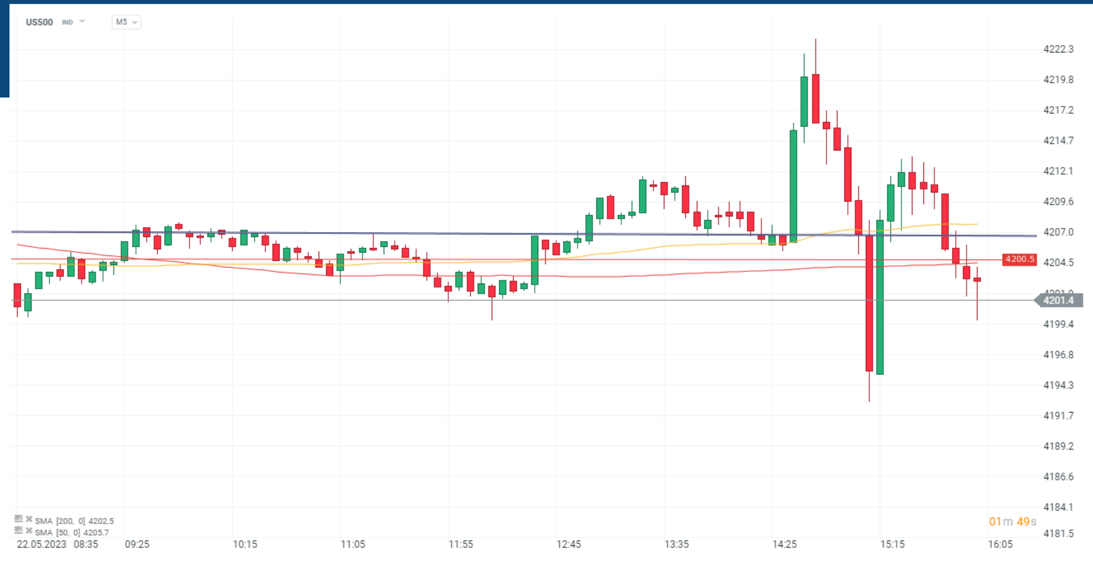
And send the correct amount to the address specified in this window.

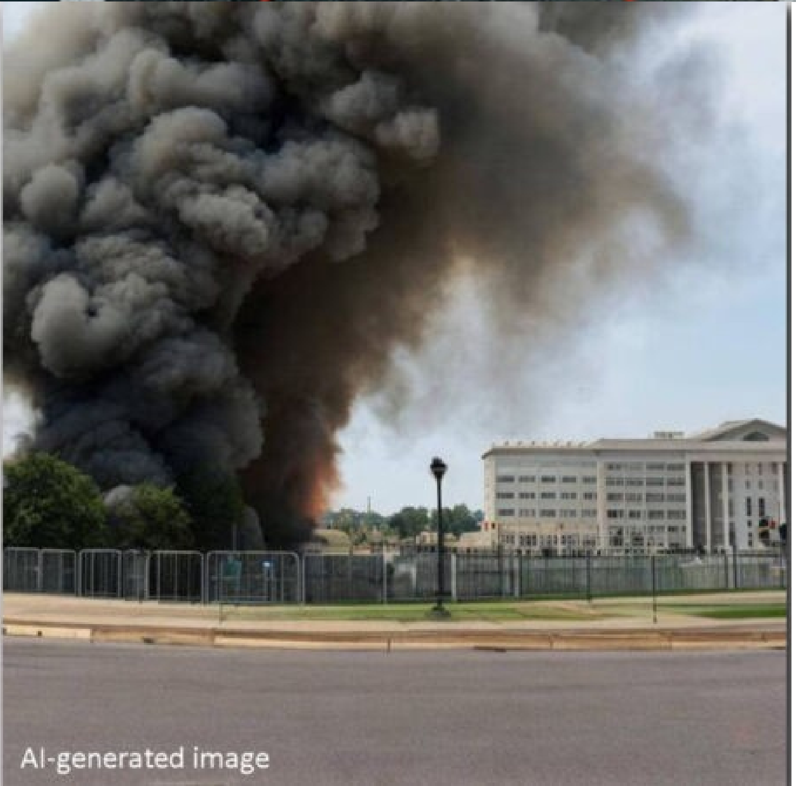
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

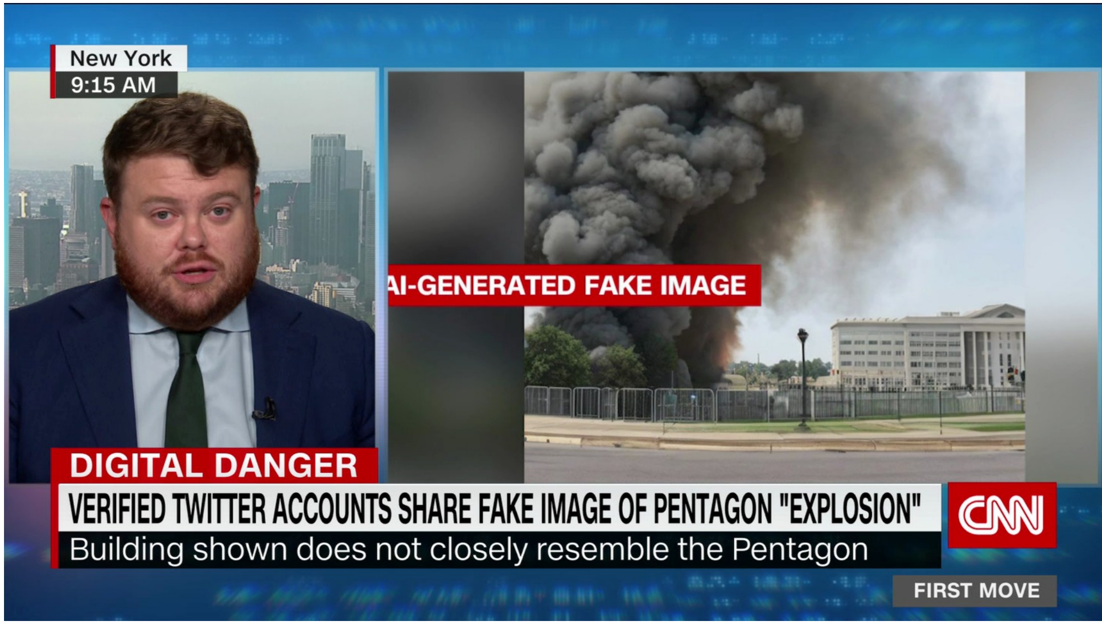

Explosion near the #Pentagon building

Follow @CBKNEWS121

#America #MAGA




AI-generated image



DIGITAL DANGER

VERIFIED TWITTER ACCOUNTS SHARE FAKE IMAGE OF PENTAGON "EXPLOSION"

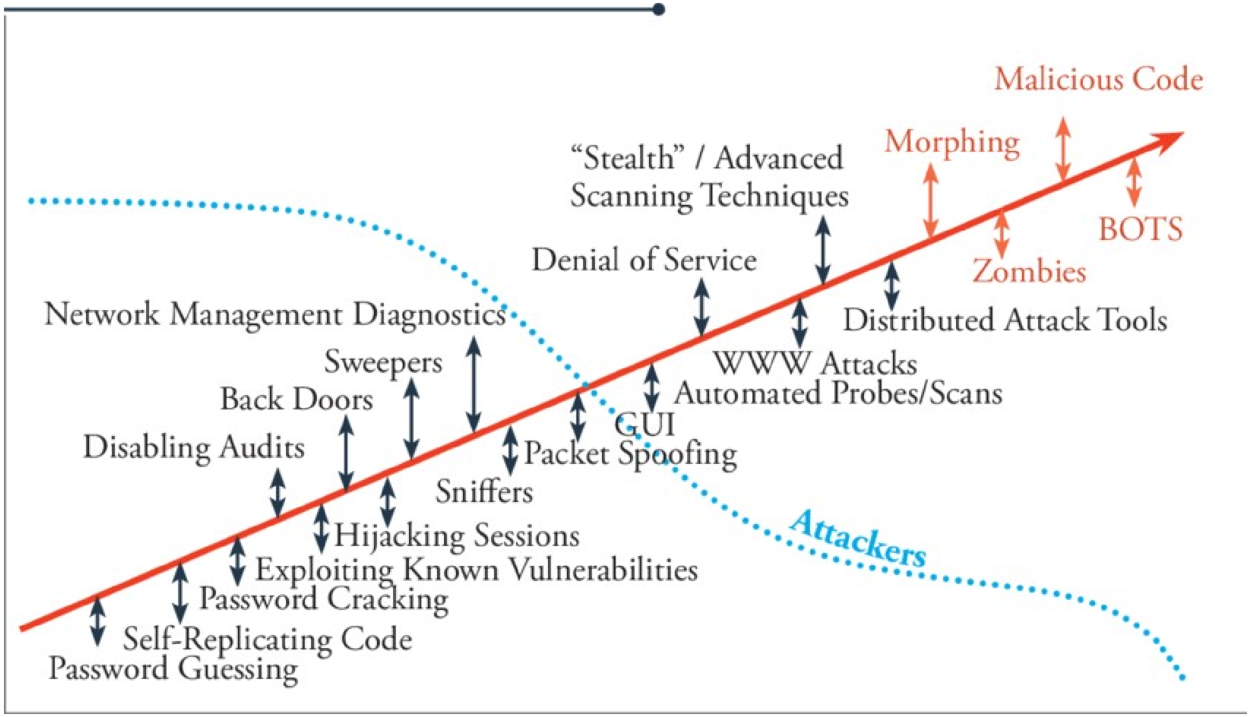
Building shown does not closely resemble the Pentagon

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

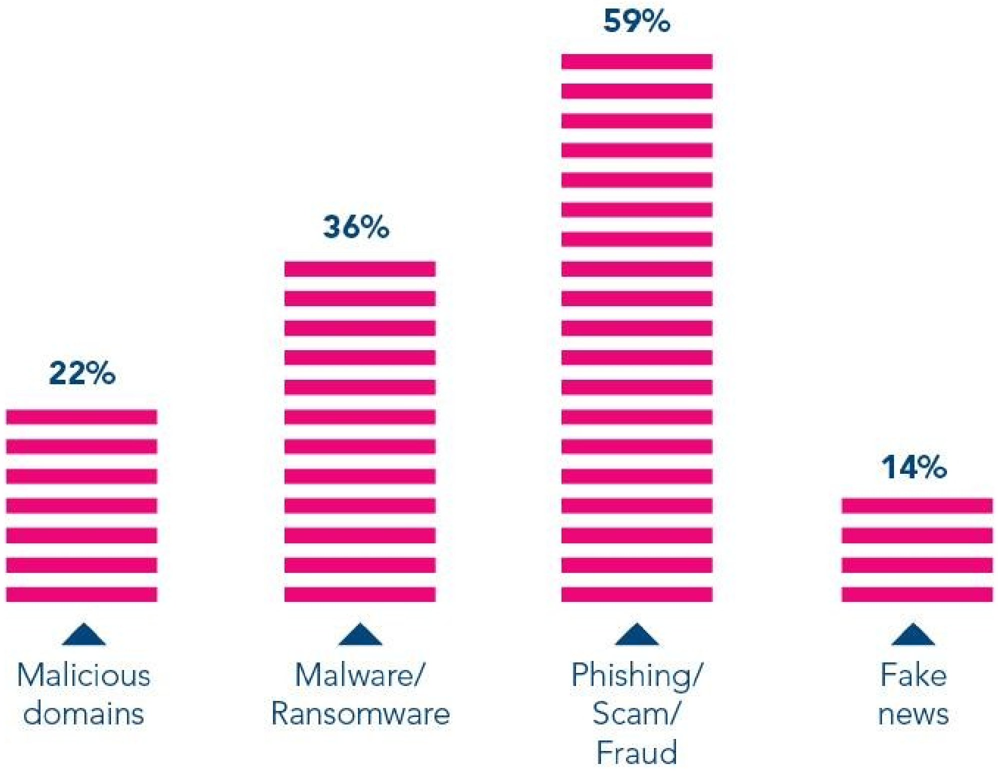
The Evolution of Cybersecurity

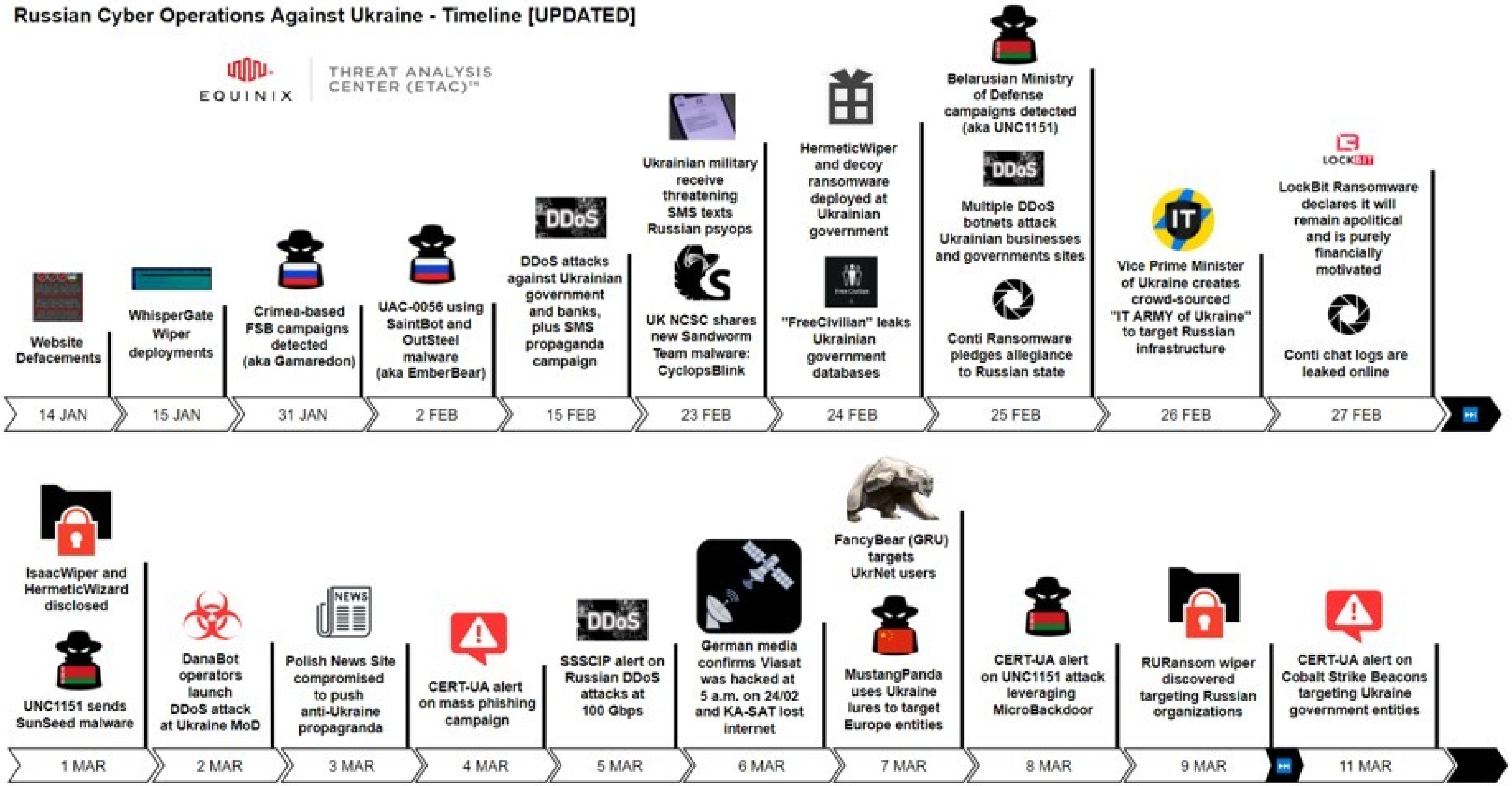
Cybersecurity is no longer a technological ‘option’, but a societal need and a value. Examples:

- 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





Russian Cyber Operations Against Ukraine - Timeline [UPDATED]

EQUINIX | THREAT ANALYSIS CENTER (ETAC)™

14 JAN – Website Defacements

15 JAN – WhisperGate Wiper deployments

31 JAN – Crimea-based FSB campaigns detected (aka Gamaredon)

2 FEB – UAC-0056 using SaintBot and OutSteel malware (aka EmberBear)

15 FEB – DDoS attacks against Ukrainian government and banks, plus SMS propaganda campaign

23 FEB – Ukrainian military receive threatening SMS texts Russian psyops; UK NCSC shares new Sandworm Team malware: CyclopsBlink

24 FEB – HermeticWiper and decoy ransomware deployed at Ukrainian government; "FreeCivilian" leaks Ukrainian government databases

25 FEB – Belarusian Ministry of Defense campaigns detected (aka UNC1151); Multiple DDoS botnets attack Ukrainian businesses and governments sites; Conti Ransomware pledges allegiance to Russian state

26 FEB – Vice Prime Minister of Ukraine creates crowd-sourced "IT ARMY of Ukraine" to target Russian infrastructure

27 FEB – LockBit Ransomware declares it will remain apolitical and is purely financially motivated; Conti chat logs are leaked online

1 MAR – IsaacWiper and HermeticWizard disclosed; UNC1151 sends SunSeed malware

2 MAR – DanaBot operators launch DDoS attack at Ukraine MoD

3 MAR – Polish News Site compromised to push anti-Ukraine propagranda

4 MAR – CERT-UA alert on mass phishing campaign

5 MAR – SSSCIP alert on Russian DDoS attacks at 100 Gbps

6 MAR – German media confirms Viasat was hacked at 5 a.m. on 24/02 and KA-SAT lost internet

7 MAR – FancyBear (GRU) targets UkrNet users; MustangPanda uses Ukraine lures to target Europe entities

8 MAR – CERT-UA alert on UNC1151 attack leveraging MicroBackdoor

9 MAR – RURansom wiper discovered targeting Russian organizations

11 MAR – CERT-UA alert on Cobalt Strike Beacons targeting Ukraine government entities

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".

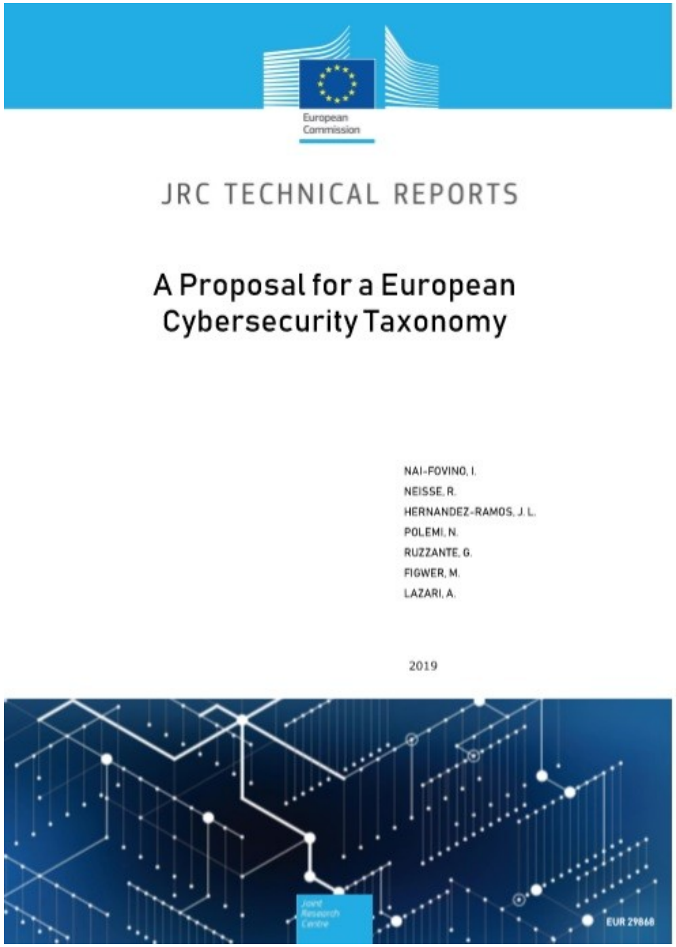
Confidentiality - Integrity - Availability

- **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.



European Commission

JRC TECHNICAL REPORTS

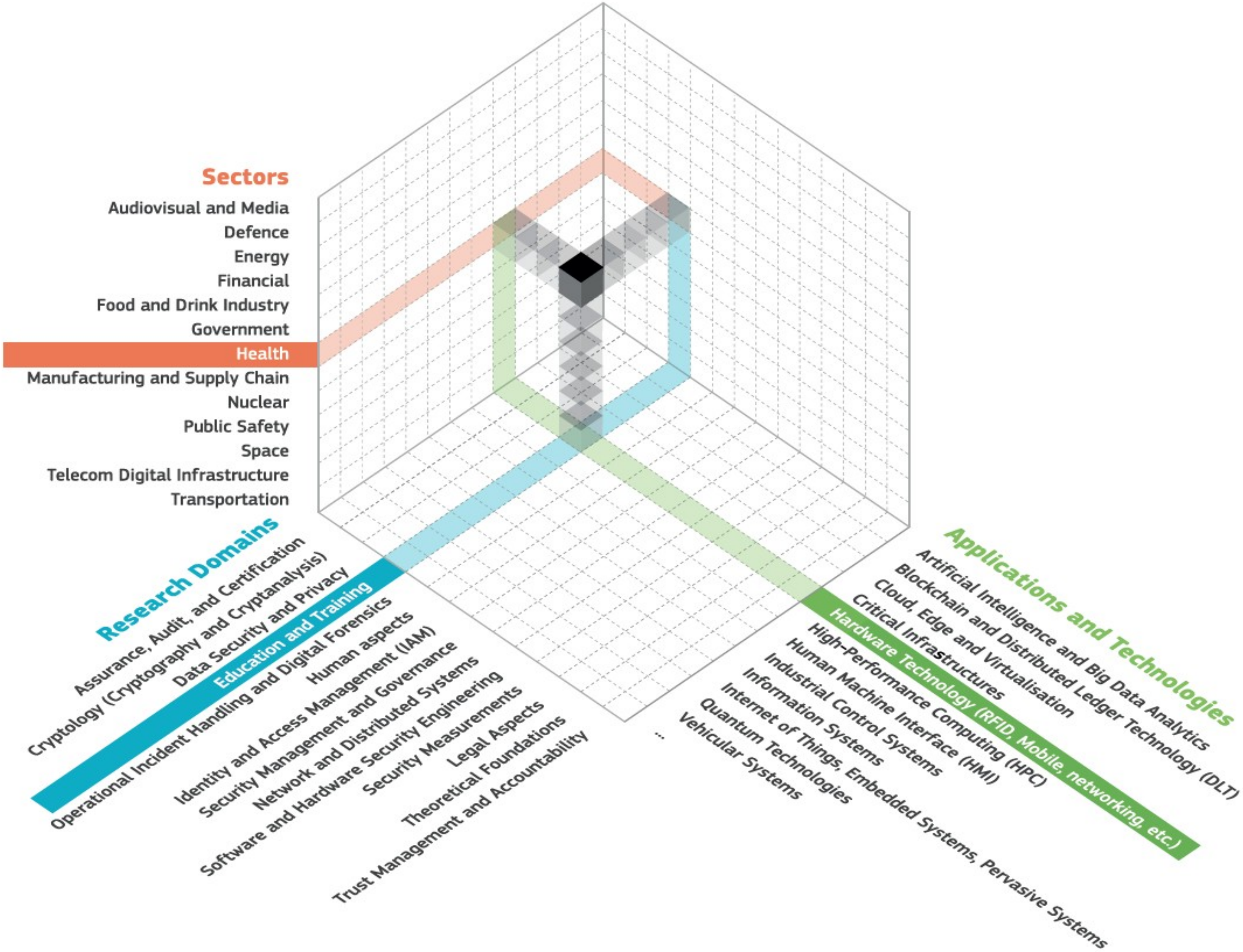
A Proposal for a European Cybersecurity Taxonomy

NAI-FOVINO, I.
NEISSE, R.
HERNANDEZ-RAMOS, J.L.
POLEMI, N.
RUZZANTE, G.
FIGWER, M.
LAZARI, A.

2019

Joint Research Centre

EUR 29868



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

- Assurance, Audit, and Certification
- Cryptology (Cryptography and Cryptanalysis)
- 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
- Hardware Technology (RFID, Mobile, networking, etc.)
- High-Performance Computing (HPC)
- Human Machine Interface (HMI)
- Industrial Control Systems
- Information Systems
- Internet of Things, Embedded Systems, Pervasive Systems
- Quantum Technologies
- Vehicular Systems
- ...

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)

20— 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

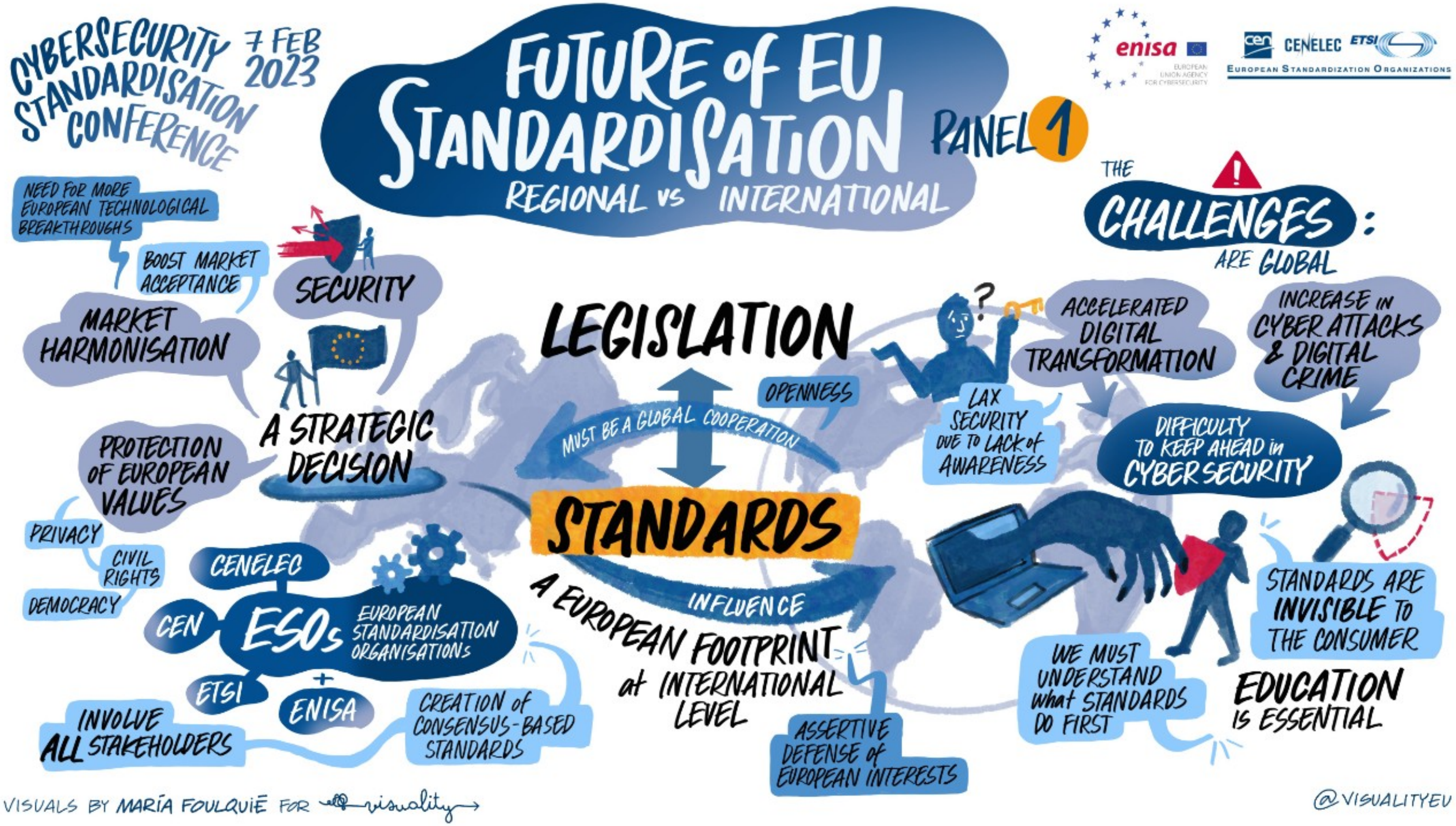
In general there is the need for:

- 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**?

Part II
The NIS Directive


CYBERSECURITY STANDARDISATION CONFERENCE
7 FEB 2023
FUTURE of EU STANDARDISATION
REGIONAL vs INTERNATIONAL
PANEL 1
enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY
cen CENELEC ETSI
EUROPEAN STANDARDIZATION ORGANIZATIONS
NEED FOR MORE EUROPEAN TECHNOLOGICAL BREAKTHROUGHS
BOOST MARKET ACCEPTANCE
SECURITY
MARKET HARMONISATION
A STRATEGIC DECISION
PROTECTION OF EUROPEAN VALUES
PRIVACY
CIVIL RIGHTS
DEMOCRACY
CENELEC
CEN
ESOs EUROPEAN STANDARDISATION ORGANISATIONS
ETSI
+
ENISA
INVOLVE ALL STAKEHOLDERS
CREATION of CONSENSUS-BASED STANDARDS
LEGISLATION
MUST BE A GLOBAL COOPERATION
OPENNESS
STANDARDS
INFLUENCE
A EUROPEAN FOOTPRINT at INTERNATIONAL LEVEL
ASSERTIVE DEFENSE of EUROPEAN INTERESTS
THE CHALLENGES : ARE GLOBAL
ACCELERATED DIGITAL TRANSFORMATION
INCREASE IN CYBER ATTACKS & DIGITAL CRIME
LAX SECURITY DUE TO LACK of AWARENESS
DIFFICULTY TO KEEP AHEAD in CYBERSECURITY
STANDARDS ARE INVISIBLE TO THE CONSUMER
WE MUST UNDERSTAND what STANDARDS DO FIRST
EDUCATION IS ESSENTIAL
VISUALS BY MARÍA FOULQUIÉ FOR visuality
@VISUALITYEU

Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace

The strategy identified the achievement of cyber-resilience and the development of industrial and technological resources for cybersecurity as its key objectives.

The Directive on Security of Network and Information Systems across the EU (the NIS Directive) represents the first piece of EU-wide legislation on cybersecurity.

NIS Directive creates

- legal measures to boost the overall level of cybersecurity in the EU, with a focus on protecting critical infrastructure.
- the NIS Cooperation Group, and the network of Computer Security Incident Response Teams (CSIRTs).
- other measures exchange of information on cybersecurity and cooperation on specific cybersecurity incidents.

Principles for Cybersecurity in the Joint Communication

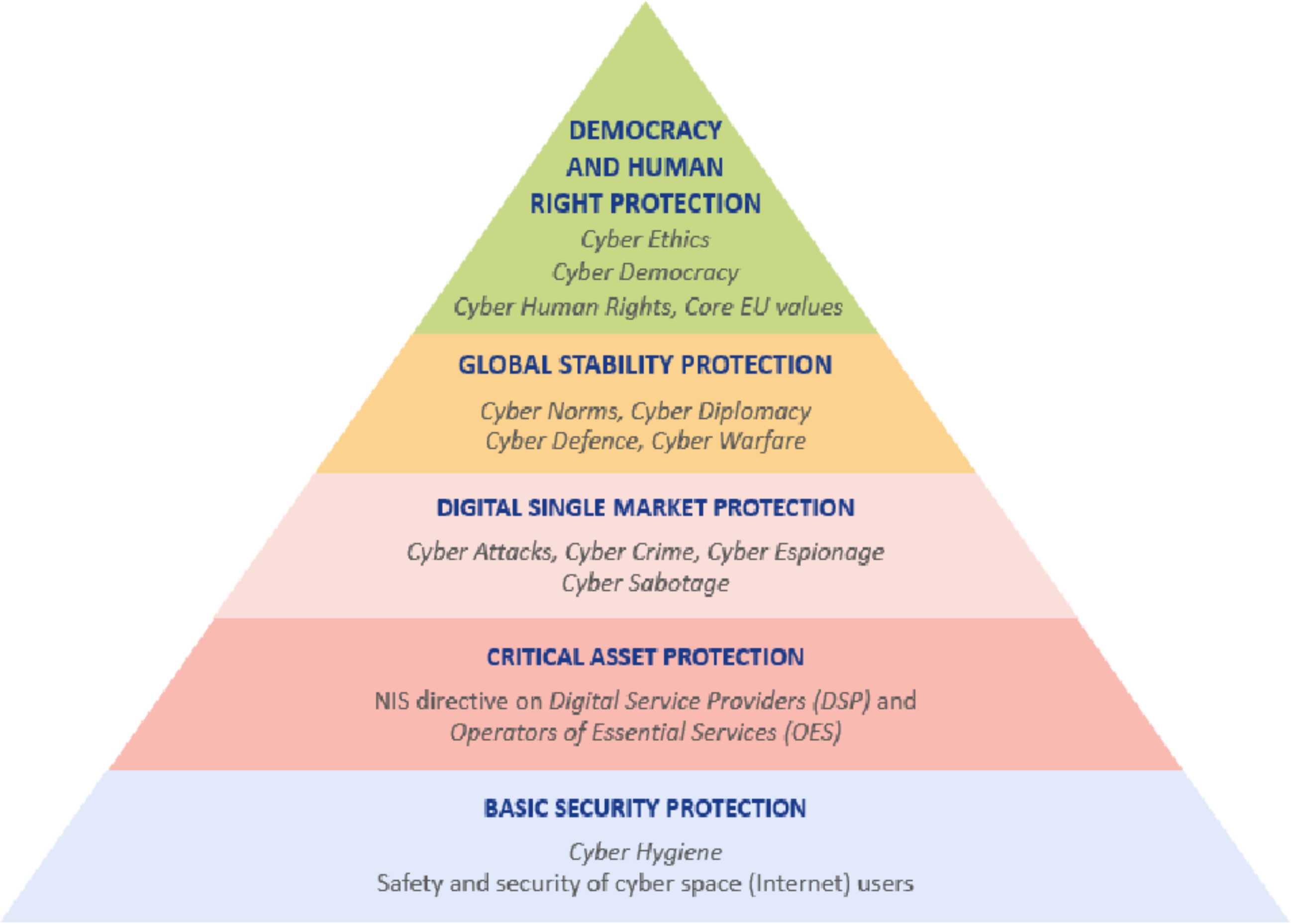
<u>The EU's core values apply as much in the digital as in the physical world</u>

- Protecting fundamental rights, freedom of expression, personal data and privacy
- Access for all - digital literacy
- Democratic and efficient multi-stakeholder governance
- A shared responsibility to ensure security

<u>Five strategic priorities</u>

- Achieving cyber resilience
- Drastically reducing cybercrime
- Developing cyberdefence policy and capabilities related to the Common Security and
- Defence Policy (CSDP)
- Develop the industrial and technological resources for cybersecurity
- Establish a coherent international cyberspace policy for the European Union and promote
- core EU values

Layers of cybersecurity protection (Enisa, 2017)



DEMOCRACY AND HUMAN RIGHT PROTECTION

Cyber Ethics
Cyber Democracy
Cyber Human Rights, Core EU values

GLOBAL STABILITY PROTECTION

Cyber Norms, Cyber Diplomacy
Cyber Defence, Cyber Warfare

DIGITAL SINGLE MARKET PROTECTION

Cyber Attacks, Cyber Crime, Cyber Espionage
Cyber Sabotage

CRITICAL ASSET PROTECTION

NIS directive on *Digital Service Providers (DSP)* and *Operators of Essential Services (OES)*

BASIC SECURITY PROTECTION

Cyber Hygiene
Safety and security of cyber space (Internet) users

The NIS Directive

Adoption: 6 July 2016
Transposition: 9 May 2018

The EU’s Directive on security of network and information systems (NIS Directive) is part of the legislated response to cyber threats.

It aims to achieve a high common level of network and information system security – in particular availability – across the EU by:

- Improving national cyber security capabilities;
- Increasing cooperation between member states; and
- Requiring **operators of essential services** (OES) and **digital service providers** (DSPs) to take appropriate and proportionate security measures, and notify the relevant national authorities of serious incidents.

The Difficult Transposition of the NIS Directive

“Member States should take appropriate measures to ensure that the provisions and the cooperation models of the NIS Directive can provide the best possible EU-level tools to achieve a high common level of security of network and information systems across the Union. The Commission invites Member States to consider in this process the relevant information, guidance and recommendations contained in this Communication.”

- The Development of a National Strategy

- By 2020, all member states had communicated to the Commission the transposition of the NIS Directive into their national legislation.

The NIS Directive - Four principal goals

1. Manage security risks;
2. Protect against cyber attacks;
3. Detect cybersecurity events;
4. Minimize the impact of cybersecurity incidents.

Risks are defined as “any reasonably identifiable circumstances or events having a potential adverse effect on the security of network and information systems”.

The NIS Directive - Legal basis

Question:
Does the EU have a mandate to act in this field without the Treaties providing **any real competence** in cybersecurity?

The European Union is based on the **rule of law**. This means that every action taken by the EU is founded on treaties that have been approved democratically by its members. EU laws help to achieve the objectives of the EU treaties and put EU policies into practice.

The term "**legal basis**" refers to the part of one of the EU's treaties (most commonly in the Treaty on the Functioning of the European Union - TFEU) that gives the EU the legal right to act.

The NIS Directive - Legal basis

Consequences:

1. If there is no basis in one of the treaties for EU action on an issue then the EU cannot enact legislation on that issue.

2. In the absence of a specific legal basis, the Union can act on the basis of Article 352 TFEU (unanimity in the Council and simple consultation of EP).

The cybersecurity legislation has been proposed and approved by relying on the "**internal market harmonisation**" legal basis, i.e., Art. 114 TFEU.

The NIS Directive - Legal basis

Art. 114 TFEU

“Save where otherwise provided in the Treaties, the following provisions shall apply for the achievement of the objectives set out in Article 26. The European Parliament and the Council shall, acting in accordance with the ordinary legislative procedure and after consulting the Economic and Social Committee, adopt the measures for the approximation of the provisions laid down by law, regulation or administrative action in Member States which have as their object the establishment and functioning of the internal market.

[...]

3. The Commission, in its proposals envisaged in paragraph 1 concerning health, safety, environmental protection and consumer protection, will take as a base a high level of protection, taking account in particular of any new development based on scientific facts. Within their respective powers, the European Parliament and the Council will also seek to achieve this objective”

The NIS Directive - Legal basis

The use of Art. 114 TFEU to pursue cybersecurity initiatives **did not come without controversy**.

In 2006, the **United Kingdom** contested the use of the internal market competence for the establishment of the European Network and Information Security Agency (ENISA).

During the years, Member States have pointed out the limits of Art. 114 TFEU to pursue additional policy objectives other than the harmonisation of the internal market. Often, Art. 352 TFEU was proposed as a possible alternative to the use of 114 TFEU.

The NIS Directive and EU landscape

The Commission’s efforts for the broader digitisation of Europe are outlined in its policy initiative “Europe’s Digital Decade 2030”.

The language used in this communication clearly pitches “Europe” as paving its own way to the digital realm on a variety of topics, from Artificial Intelligence to data sharing, from hyper connected devices to quantum computing.

Europe’s decade is juxtaposed to developments in, say, the USA and China. The underlying idea is that only a united Europe, with a **holistic approach to digital development**, can and will be able to cope in the global arena

Raising common security level of "NISs"

The NIS Directive:

- lays down obligations on all Member States to adopt a national strategy on network and information systems security;
- creates a Cooperation Group to support and facilitate strategic cooperation and the exchange of information among Member States and foster trust and confidence amongst them;
- creates a network of Computer Security Incident Response Teams (CSIRTs network) to further contribute to the growth of trust and confidence;
- establish security and notification requirements for operators of essential services and digital service providers;
- lays down obligations for Member States to designate national competent authorities, single points of contact and CSIRTs.

Elements of Member State's national strategies

- The objectives and priorities of the NIS (network and information systems) security strategy.
- A governance framework to achieve these objectives and priorities, including roles and responsibilities for government bodies and other actors.
- Identification of measures relating to preparedness, response and recovery, including cooperation between the public and private sectors.
- An indication of the education, awareness-raising and training programmes on the NIS security strategy.
- An indication of the research and development plans relating to the NIS security strategy
- An assessment plan to identify potential risks.
- A list of the various actors involved in the implementation of the NIS security strategy.

States must create **Computer security incident response teams** (CSIRT)

Who is considered an OES?

The NIS Regulations deem the following sectors offer essential services:

- **Energy** Electricity, oil and gas.
- **Transport** Air, rail, water and road.
- **Health care** settings (including hospitals, private clinics and online settings).
- **Water** Drinking water supply and distribution.
- **Digital infrastructure** Top-level domain (TLD) name registries, domain name systems (DNS) service providers and Internet exchange point (IXP) operators.

The NIS Directive require Member States to identify OESs.

Who is considered a DSP?

The NIS Regulations define DSPs as “any person who provides a digital service”. However, ‘micro and small enterprises’ do not fall under the scope of the Regulations. 4 Section 1(2) of the NIS Regulations identifies the following types of digital service:

- **Online search engines** “a digital service that allows users to perform searches of, in principle, all websites or websites in a particular language on the basis of a query on any subject in the form of a keyword, phrase or other input and returns links in which information related to the requested content can be found”.

- **Online marketplaces** “a digital service that allows consumers and/or traders [...] to conclude online sales or service contracts with traders either on the online marketplace’s website or on a trader’s website that uses computing services provided by the online marketplace”.

- **Cloud computing services** “a digital service that enables access to a scalable and elastic pool of shareable computing resources”, including ‘Infrastructure as a Service’ (IaaS), ‘Platform as a Service’ (PaaS) and ‘Software as a Service’ (SaaS).

Key requirements

Both OESs and DSPs face two main requirements under the NIS Regulations:

1. **Putting** “appropriate and proportionate” technical and organisational measures in place to manage the risks that might impact the availability of their essential service (Sections 10 and 12(1)).

2. **Notifying** their competent authority of any incident of “significant” or “substantial” impact (Sections 11 and 12(3)).

Appropriate and proportionate measures

The first requirement establishes the need for a minimum level of security and the ability to respond to incidents when they occur. These measures should help ensure the continuity of the essential service.

Security measures must be "appropriate to the risk".

Such measures should also consider both technical and organisational approaches.

In addition, DSPs are also explicitly required to take business continuity management into account 10 and keep "adequate documentation" that demonstrates their compliance with the Rules.

Incident reporting for OES

OES need to ensure that they notify their competent authority within 72 hours of becoming aware of a ‘significant’ incident, as stipulated by the Regulations. The Regulations also define the three parameters for determining what constitutes a “significant impact”:

1. The number of users affected.
2. The duration of the disruption.
3. The size of the affected geographical area.

OES are expected to consider all three factors in determining whether or not an incident is “significant”; competent authorities should have defined more detailed thresholds for their sector.

Note that the Regulations’ incident reporting requirements are not limited to cyber security, but include any incidents that affect the security of network and information systems, including physical events such as natural disasters.

Incident reporting for DSPs

The NIS Regulations also require DSPs to report incidents within 72 hours if they have a "substantial impact" (Section 12(3)). The Implementing Regulation makes clear that the DSP itself must determine this, and outlines the following metrics in Article 3 for determining if an incident has a "substantial" impact on the EU:

1. Service unavailability for more than 5 million user hours.
2. Loss of confidentiality, integrity, availability or authenticity of data accessed over networks or information systems affecting more than 100,000 users.
3. Incident creates a risk to public safety, public security or loss of life.
4. Material damage to at least one user exceeds €1 million (about £900,000).

If any of these apply, the DSP needs to contact the relevant authorities, who will investigate. Although DSPs are generally not closely supervised, authorities could take action when provided with evidence that the DSP may not be complying with the Regulations, particularly after an incident has occurred.

ENISA's Technical Guidelines

For DSPs, the European Union Agency for Cybersecurity (ENISA) has provided Technical Guidelines on the security measures they must implement.

The **Technical Guidelines** describe 27 security objectives, which we have arranged into broad categories in the Appendix. The Guidelines recognise that different organisations need different levels of maturity depending on their specific circumstances: each objective can be achieved at three distinct 'sophistication levels', in accordance with the results of a risk assessment.

ENISA has also provided guidance for DSPs on reporting incidents.

This explains how the overall incident notification works at EU level: again, because digital services are likely to be used remotely, a service disruption may well have a cross-border impact.

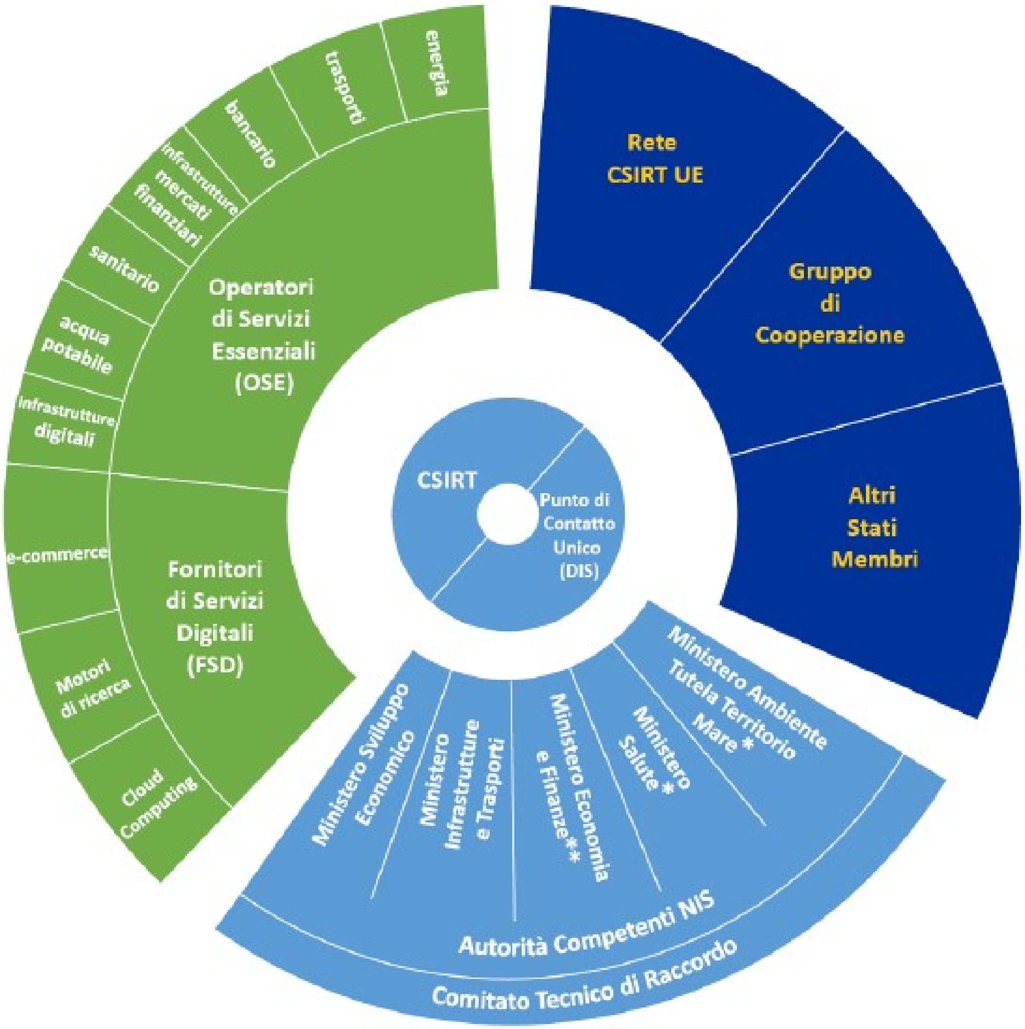
Question

Is the different approach towards digital service providers and operators of essential services **well justified**?

ENISA (2017 incident notifications for DSPs in the context of the NIS Directive paper) observes that:

"In this respect, the light-touch approach aims at avoiding overburdening the DSPs while not hampering the capacity of the EU to react to cybersecurity incidents in a swift and efficient manner".

The Nis Directive - Entities


energia
trasporti
bancario
infrastrutture mercati finanziari
sanitario
acqua potabile
infrastrutture digitali
Operatori di Servizi Essenziali (OSE)
e-commerce
Motori di ricerca
Cloud Computing
Fornitori di Servizi Digitali (FSD)
CSIRT
Punto di Contatto Unico (DIS)
Rete CSIRT UE
Gruppo di Cooperazione
Altri Stati Membri
Ministero Sviluppo Economico
Ministero Infrastrutture e Trasporti
Ministero Economia e Finanze**
Ministero Salute *
Ministero Ambiente Tutela Territorio Mare *
Autorità Competenti NIS
Comitato Tecnico di Raccordo

🟩 Servizi interessati

🟦 Attori governativi NIS

🟦 Meccanismi della cooperazione europea

* più regioni e province autonome di Trento e di Bolzano

** in collaborazione con le autorità di vigilanza di settore, Banca d'Italia e Consob

The National Cybersecurity Perimeter

Mandatory notifications in case of cyber incidents have been extended In order to **strengthen the National Cybersecurity Perimeter**. Therefore, ACN has developed the expected taxonomy of this additional type of cyber incident to make its notification and impact assessment process easier. The notification process, to be completed within 72 hours, concerns all the other IT assets of the subjects included in the Perimeter.

To implement the amendment in the decree which modifies the legal provisions relating to the Perimeter of National Cybersecurity (article 1, paragraph 3-bis of the decree-law n. 105 of 2019), it becomes **mandatory to also notify incidents** that impact networks, systems and information services that are not directly assigned under the Perimeter itself. This means that **even an attempt to access other IT assets** other than those protected by the Perimeter **must be reported** to the Computer Security Incident Response Team (CSIRT Italia) of the National Cybersecurity Agency of Italy (ACN.

The role of ENISA

(a) anticipate and support Europe in facing emerging network and information security challenges;

(b) promote network and information security as an EU policy priority;

(c) support Europe in maintaining state of the art NIS capacities;

(d) foster the emerging European NIS Community.

See. ENISA Strategy 2022-2024.

At the same time ENISA actively assists the competent authorities by appointing its representative in the Cooperation Group and by providing the secretariat in the CSIRTs network.

The Cybersecurity Act (Reg. 2019/881)

The Cybersecurity Act strengthens the EU Agency for cybersecurity (ENISA) and establishes a cybersecurity certification framework for products and services.

ENISA will have a key role in setting up and maintaining the European cybersecurity certification framework by preparing the technical ground for specific certification schemes. It will be in charge of informing the public on the certification schemes and the issued certificates through a dedicated website.

ENISA is mandated to increase operational cooperation at EU level, helping EU Member States who wish to request it to handle their cybersecurity incidents, and supporting the coordination of the EU in case of large-scale cross-border cyberattacks and crise

The EU Cybersecurity Act introduces an E**U-wide cybersecurity certification framework** for ICT products, services and processes. Companies doing business in the EU will benefit from having to certify their ICT products, processes and services only once and see their certificates recognised across the European Union.

The EU cybersecurity certification framework

The **certification** will attest that ICT products and services that have been certified in accordance with such a scheme comply with specified requirements.

In particular, each European scheme should specify:

- the categories of products and services covered;
- the cybersecurity requirements, such as standards or technical specifications;
- the type of evaluation, such as self-assessment or third party;
- the intended level of assurance.

The assurance levels are used to inform users of the cybersecurity risk of a product, and can be **basic**, **substantial**, or **high**. They are commensurate with the level of risk associated with the intended use of the product, service or process, in terms of probability and impact of an accident.

The resulting certificate will be recognised in all EU Member States, making it easier for businesses to trade across borders and for purchasers to understand the security features of the product or service.

Advising and supporting ENISA: ECCG & SCCG

As for the implementation of the certification framework, Member State authorities, gathered in the **European Cybersecurity Certification Group (ECCG)** have already met several times.

Following the entry into force of the Cybersecurity Act in 2019, the European Commission launched a call for applications to select members of the **Stakeholder Cybersecurity Certification Group (SCCG)**.

The SCCG will be responsible for advising the Commission and ENISA on strategic issues regarding cybersecurity certification, and assisting the Commission in the preparation of the Union rolling work programme. This is the first stakeholder expert group for cybersecurity certification launched by the European Commission.

Evaluation of the functioning of the NIS Directive

The evaluation on the functioning of the NIS Directive identified the following issues:

- the **low level of cyber resilience** of businesses operating in the EU;
- the **inconsistent resilience** across Member States and sectors;
- the **low level of joint** situational awareness and lack of joint crisis response.

The scope of the NIS Directive is too limited in terms of the sectors covered, mainly due to:

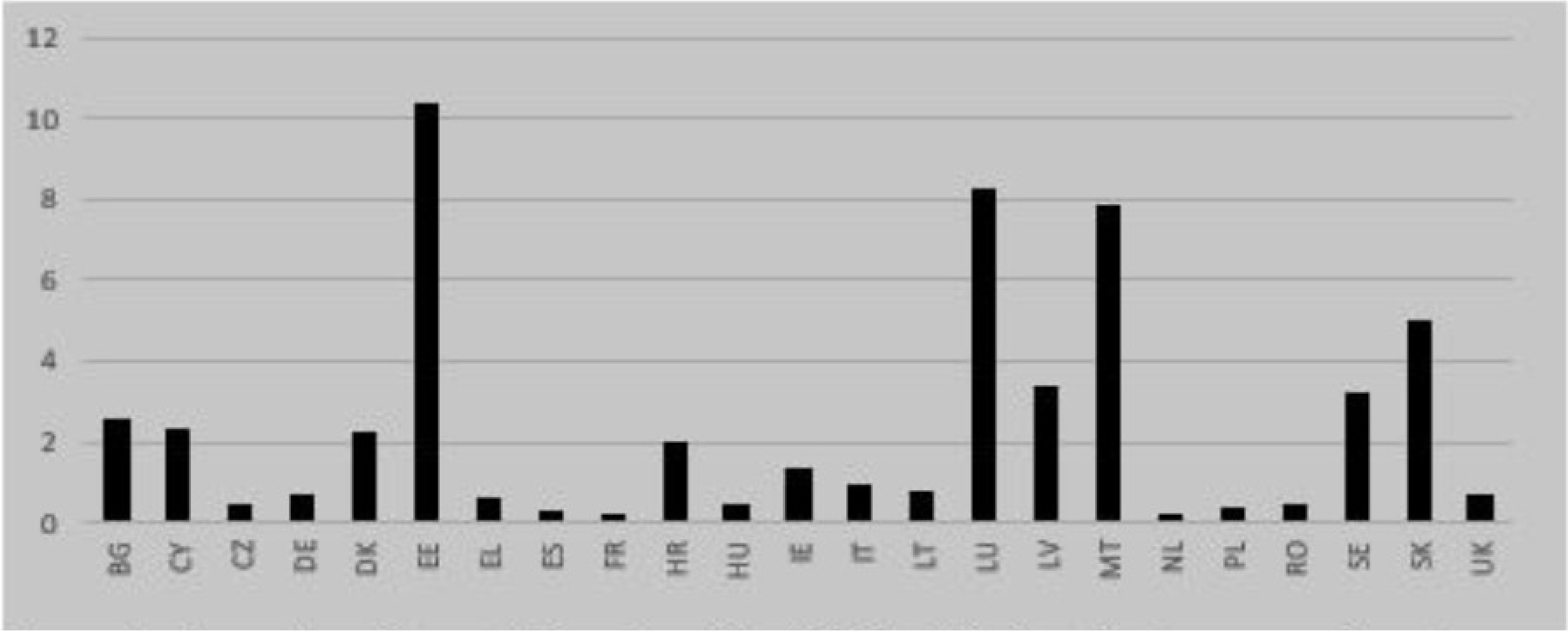
- increased digitisation in recent years and a higher degree of interconnectedness;
- the scope of the NIS Directive no longer reflecting all digitised sectors providing key services to the economy and society as a whole.

Evaluation of the functioning of the NIS Directive

The NIS Directive **is not sufficiently clear** when it comes to the scope for OESs and its provisions do not provide sufficient clarity regarding national competence over digital service providers. This has led to a situation in which certain types of entities have not been identified in all Member States and are therefore not required to put in place security measures and report incidents.

The NIS Directive allowed **wide discretion** to the Member States when laying down security and incident reporting requirements for operators of essential services (OESs). The evaluation shows that in some instances Member States have implemented these requirements in significantly different ways, creating additional burden for companies operating in more than one Member State.

The number of OESs identified across the EU



OESs identified by Members States across all sectors per 100.000 inhabitants (source European Commission, 2020)

Evaluation of the functioning of the NIS Directive

The supervision and enforcement regime of the NIS Directive is **ineffective**. For example, Member States have been very reluctant to apply penalties to entities failing to put in place security requirements or report incidents.

The financial and human resources set aside by Member States for fulfilling their tasks (such as OES identification or supervision), and consequently the different levels of maturity in dealing with cybersecurity risks, vary greatly. This further exacerbates the differences in cyber resilience between Member States.

Member States do not share information systematically with one another, with negative consequences in particular for the effectiveness of the cybersecurity measures and for the level of joint situational awareness at EU level.

Preparation of the (new)proposal - OPC

To underpin the proposal and collect evidence, the Commission ran an **open public consultation** (OPC), launched stakeholder interviews, country visits, workshops and surveys, carried out a study on NIS investment and an impact assessment, and drew up a roadmap.

The OPC was carried out over a **12-week period**, starting on 7 July 2020 and closing on 2 October 2020. A total of 206 replies were collected online, 182 of which were from respondents located in the EU-27.

Impact assessment

The Commission conducted an impact assessment (IA), comprising three different documents.

The IA explored four different policy options for the NIS review, including the baseline option:

0) maintaining the status quo;

1) non-legislative measures to align the transposition;

2) limited changes to the NIS Directive for further harmonisation;

3) **systemic and structural changes to the NIS Directive.**

2020 Cybersecurity Strategy

On **16 December 2020**, the European Commission and the High Representative of the Union for Foreign Affairs and Security Policy presented a new EU Cybersecurity Strategy

- bolster Europe’s collective resilience against cyber threats
- ensure that all citizens and businesses can fully benefit from trustworthy and reliable services and digital tools.

The Commission made two new proposals, by now both adopted:

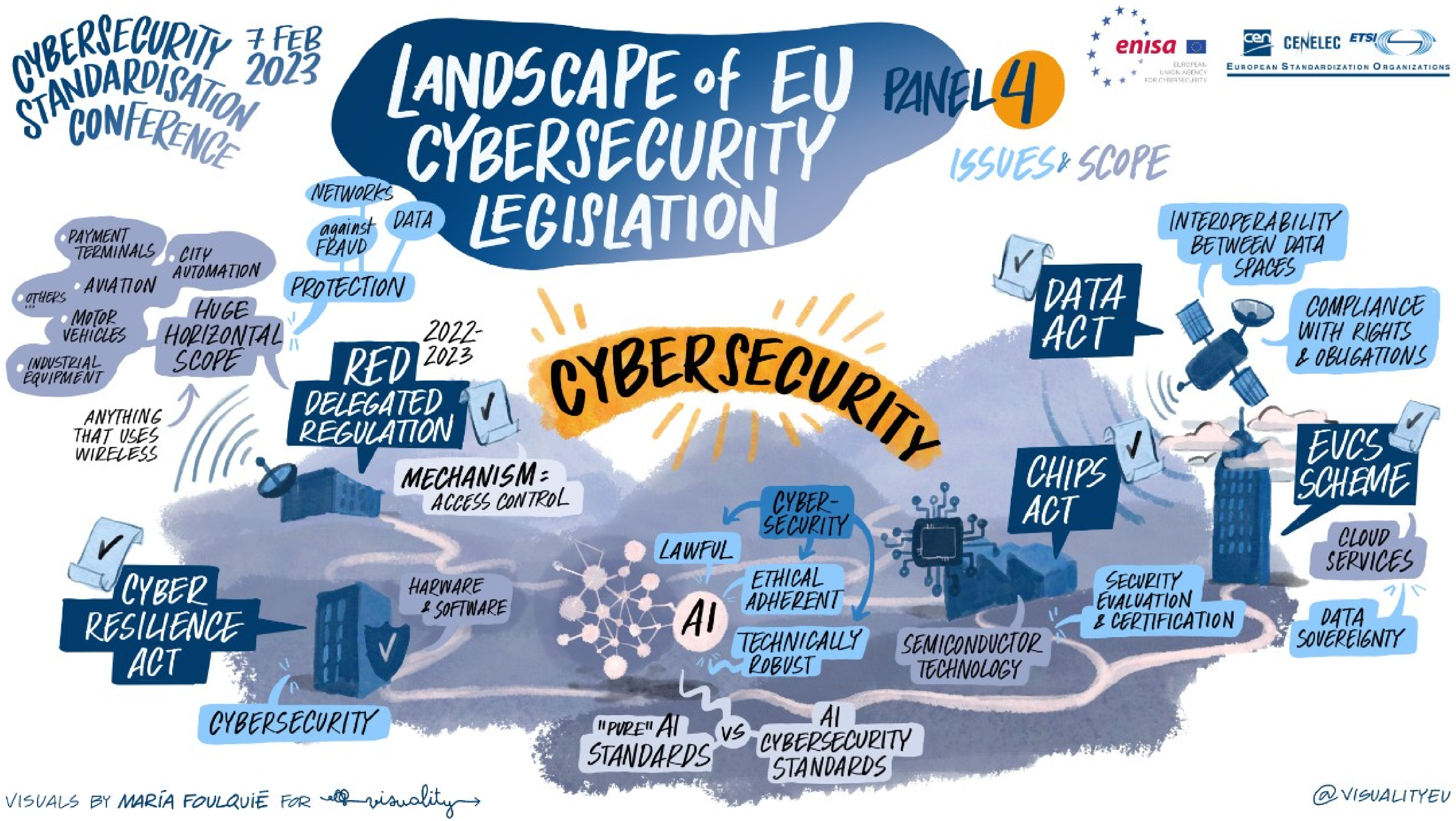
- a Directive on measures for high common level of cybersecurity across the Union (see related wagon ‘NIS 2');
- a new Directive on the resilience of critical entities.

The Design of Next Steps

- 22 March 2021 the European Council adopted its conclusions on the cybersecurity strategy with the work of the coming years
- 10 June 2021, Parliament calls for connected products and associated services, including supply chains, to be made secure-by-design, resilient to cyber incidents, and quickly patched if vulnerabilities are discovered
- 15 September 2021, the Commission's president announced an initiative to create an European Cyber Defence Policy with roadmap on security and defence technologies
- 22 March 2022, the Commission proposed a Regulation to establish common cybersecurity measures across the European Union institutions, bodies, offices and agencies
- 9 March 2022 European governments adopted a declaration to reinforce the EU's cybersecurity capacities, including establishing a new fund and increasing EU funding to support national efforts.
- 21 June 2022 the Council adopted the Framework for a coordinated EU response to hybrid campaigns
- 15 September 2022 the Commission presented a legislative proposal known as the EU Cyber Resilience Act
- 18 October 2022 the Commission announced in its Work programme 2023 a non-legislative initiative to establish the Cybersecurity e-skills academy in Q3 2023.

Part III

Security obligations in other EU legislation


CYBERSECURITY STANDARDISATION CONFERENCE
7 FEB 2023
LANDSCAPE of EU CYBERSECURITY LEGISLATION
PANEL 4
ISSUES & SCOPE
enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY
cen CENELEC ETSI
European Standardization Organizations
NETWORKS
against FRAUD
DATA
PROTECTION
PAYMENT TERMINALS
CITY AUTOMATION
AVIATION
OTHERS ...
MOTOR VEHICLES
INDUSTRIAL EQUIPMENT
HUGE HORIZONTAL SCOPE
ANYTHING THAT USES WIRELESS
2022-2023
RED DELEGATED REGULATION
MECHANISM = ACCESS CONTROL
CYBERSECURITY
CYBER RESILIENCE ACT
HARWARE & SOFTWARE
CYBERSECURITY
CYBER-SECURITY
LAWFUL
ETHICAL ADHERENT
AI
TECHNICALLY ROBUST
"PURE" AI STANDARDS
VS
AI CYBERSECURITY STANDARDS
DATA ACT
INTEROPERABILITY BETWEEN DATA SPACES
COMPLIANCE WITH RIGHTS & OBLIGATIONS
CHIPS ACT
SEMICONDUCTOR TECHNOLOGY
SECURITY EVALUATION & CERTIFICATION
EUCS SCHEME
CLOUD SERVICES
DATA SOVEREIGNTY
VISUALS BY MARÍA FOULQUIÉ FOR visuality
@VISUALITYEU

GDPR

Data minimization	Recitals 28, 39, 83; Articles 5.1.c, 25.1; 32.1.a	**Organizational measures** • Identification of data strictly necessary for processing purposes **Technical measures** • Systems and services that minimize data collection and use of personal data
Data storage limitation	Recital 39; Article 5.1.e	**Organizational measures** • Definition of relevant data retention periods **Technical measures** • Systems for automatic periodic data deletion
Data confidentiality	Recitals 28, 39, 83; Articles 5.1.c, 5.1.f, 25, 32.1.a, 32.1.b, 32.1.4	**Organizational measures** • Security policy • Records of processing activities **Technical measures** • Hiding personal data and their relationships • Access control to database and services • Server and database security/network and communication security • Physical system security

From: Mantelero et al 2020

GDPR

Risk assessment and security measures	Recitals 84, 90 Articles 30, 32, 35	**Organizational measures** • Risk analysis and DPIA, including technical and organizational measures
Data protection by design and by default	Recital 78 Article 25	**Organizational measures** • Adoption of specific security requirements and procedures from the early stages of the development lifecycle • Procedures to integrate data protection safeguards into processing activities **Technical measures** • Special technologies to support privacy and data protection (PETs)
Regular assessment of the effectiveness of the security measures adopted	Article 32.1.d	**Organizational measures** • Records of technical and organizational security measures taken **Technical measures** • Vulnerability and penetration testing

From: Mantelero et al 2020

GDPR

Notifications, reporting obligations, and mitigation measures (data breaches)	Recitals 85, 86, 87 Articles 33, 34	**Organizational measures** • Procedures to immediately detect whether a personal data breach has taken place • Incident response plan **Technical measures** • Data flow and log analysers • Tokenization, encryption, etc.
Business Continuity, Disaster Recovery, and resilience	Article 32.1.b, 32.1.c	**Organizational measures** • Business continuity plan • Data restore procedures • Adoption of an effective cyber-resilience approach • Disaster recovery plan **Technical measures** • Backup techniques • Business continuity technologies (eg redundancy techniques)

From: Mantelero et al 2020

eIDAS

Risk assessment and security measures	Article 19	**Technical measures** Authentication factors, which fall into the following categories: • Knowledge-based factors (eg PINs, passwords, memorable words or dates, pass phrases, pre-registered knowledge and other information likely to be known only to the subject) • Possession-based factors (eg asymmetric cryptographic (private) keys, where the private keys may be stored on dedicated hardware devices (eg smartcards), or software tokens, uniquely identifiable tokens (eg the SIM card of a cell phone) or devices with one-time-passwords, eg 'RSA-Tokens' or printed cards) • Biometric factors (eg fingerprints, palm prints, palm veins, face, hand geometry, iris, etc)
Data protection by design and by default	Article 12.3.c	**Technical measures** • Software development has inspired the use of a catalogue of precise design patterns to develop solutions to known security problems. • Risk management frameworks and engineering objectives highlight a privacy risk model and three privacy system objectives (on top of the classic security objectives represented by confidentiality, integrity and availability): predictability, manageability and disassociability (US NIST).

From: Mantelero et al 2020

eIDAS

Notifications, reporting obligations, and mitigation measures	Recitals 31, 38, 39 Article 19.2	**Organizational measures** • Notification can be of the user or by publishing the required information on the provider's website depending on the nature of the breach, using applications or software to provide a document or fill in a form to notify providers of any incidents.
Business Continuity, Disaster Recovery, and resilience	Article 10.3 Article 24.2.h and 24.2.i	**Organizational measures** • Business impact analysis and threat analysis (to identify events that could cause an interruption of business operations and processes). • Following threat identification, a risk assessment must be performed to determine the impact of the threat on the business, likelihood of occurrence, and recovery time necessary for essential business applications and processes. • All these activities must be performed with the full involvement of the owners of the business data and business processes, and using new technologies such as: risk management, vulnerability management, identification and prioritization of business processes and supporting applications, etc.

From: Mantelero et al 2020

eIDAS

Certification process	Recitals 44 Recital 55	**Organizational measures** • Assessment of Standards related to eIDASb: ENISA sets out aspects of qualified electronic signature creation devices (QSCD certification) and qualified trust services providers (QTSP supervision) showing how to combine the respective elements in line with the eIDAS requirements. **Technical measures** • ENISAc seeks to support standards CEN EN 419 241-2 and CEN EN 419 221-5:2018 so that they could be referenced in an amended version of CID (EU) 2016/650.
Annual report to the European Authority	Article 19.3 (report to ENISA)	**Organizational measures** • The supervisory body must provide ENISA with an annual report on security breach and loss of integrity notifications received from trust service providers. **Technical measures** • Various technical measures should be developed to facilitate reporting on the vital infrastructure of the digital society, electronic communication networks and services: ● applications or open source software for quick and easy reporting ● technologies to classify annual incidents ● sets of capabilities for sector and industry clusters.

From: Mantelero et al 2020

NIS

Risk assessment and security measures	Recital 49 Article 14.1, 14.2 and Article 16.1 and 16.2	**Technical measures** • Communication (email) risk assessment (Domain Keys Identified Mail, Sender Policy Framework, Domain-based Message Authentication, Reporting and Conformance) • Software management • Access control • Authentication factors
Notifications, reporting obligations, and mitigation measures	Article 9. 4 Article 14.3 and 14.4 Article 16.3 and 16.4	**Organizational measures** - Providers and operators must immediately report significant disruptions to the National Agency and the reporting obligations must have no adverse effect on correcting the disruption. **Technical measures** - Technologies supporting notification and reporting obligations must: - (i) adopt alerting systems; - (ii) gather information on incidents; - (iii) provide automated completion of notifications using preestablished NIS elements (number of users affected, duration of incident, geographic spread, extent of disruption to service, impact on economic and social activity).

From: Mantelero et al 2020

NIS

Business Continuity, Disaster Recovery, and resilience	Recitals 69 Article 14.2 and Article 16.1.c	**Organizational measures** ● Operators and providers must ensure cyber-resilience, implementing business continuity management measures such as: ○ cyber risk and vulnerability management ○ incident response team ○ alternative resources in the event of crisis ○ backup systems.
Certification process Annual report to the European Authority	N/A Article 11.3.j	**Organizational measures** ● The Commission will examine, on an annual basis, the summary reports referred to in the second subparagraph of Article 10 (3) (notifications). **Technical measures** ● Adequate resources to assist in han- dling information necessary for the report ● Strong authentication channels to collect and store data on incidents to be reported ● Structural support to target and keep strictly confidential data and information on incidents ● Secure channel for information sharing with the Commission

From: Mantelero et al 2020

Workshop

1. Report what you observe happening with a certain frequency with reference to Cybersecurity in your field of work or study (**problems**).
2. For each of the occurrences you have identified, nail down the connected demands **(needs)**.
3. For each of the identified needs try to imagine a strategy to give a concrete answer to the identified problem and write down what you imagined (**likely solutions**).