CYBERSECURITY IN THE EU: AN INTRODUCTION

Gianluca Sciacca

Brief description

UNED´s Jean Monnet chair about Digital Economy in the EU presents this introductory document that provides an overview of the most relevant EU cybersecurity strategy policies and regulations published in the last decade. Its introductory character can be of great help for students and all those who want to have an initial but global idea on the subject.

With the support of the Erasmus+ Programme of the European Union

SUPERVISION:
JULIO NAVIO MARCO
Jean Monnet chairholder
619793-EPP-1-2020-1-ES-EPPJMO-CHAIR

CYBERSECURITY IN THE EU: AN INTRODUCTION

Gianluca Sciacca

ABSTRACT: European Union is aware of the need for a strong and reliable cybersecurity strategy to ensure trust in the cyberspace, and consequently, enhance the benefit from innovation, connectivity and automation, safeguarding fundamental rights and freedoms, including the rights to privacy and to the protection of personal data. This paper is an introduction to the most relevant EU cybersecurity strategy policies and regulations published in the last decade which reflect the current regulatory framework on data protection and critical infrastructure against cybersecurity risks. These regulations, along with the policy cybersecurity principles, are the pillars for building trust, security and privacy in the online environment which is the key to the economic and social development of the EU's project.

Content

Introduction

The currently pandemic crisis has shown undoubtedly how our economy depends on digital technologies, during which 40% of EU workers switched to telework, [1] with likely permanent effects on everyday life.[2] But digital technologies not only connect people: Connected devices already outnumber people on the planet, and their number is forecast to rise to 25 billion by 2025. [3]

It is easily seeing how many economic sectors such as finance, health, energy and transport rely utterly on the access and security information and communications technology infrastructure. Consequently, **the malicious targeting of critical infrastructure is a major global risk**.[4]

The latest figures clearly show the vulnerability of the digital market continuously subjected to cyber threats. As the report *"Main incidents in the EU and worldwide"*[5] by European Union Agency for Cybersecurity (ENISA) [6] reveals, the figures show the scale of the danger:

- 230.000 new strains of malware every day.
- 6 months on average is what it takes to detect a data breach.
- 71% of organizations experienced malware activity that spread from one employee to another.

---

[1] European Commission. (2020). *Telework in the EU before and after the COVID-19: where we were, where we head to.* Retrieved from https://ec.europa.eu/jrc/sites/jrcsh/files/jrc120945_policy_brief_-_covid_and_telework_final.pdf

[2] Gartner. (14 July 2020). *Gartner Survey Reveals 82% of Company Leaders Plan to Allow Employees to Work Remotely Some of the Time*. Retrieved from https://www.gartner.com/en/newsroom/press-releases/2020-07-14-gartner-survey-reveals-82-percent-of-company-leaders-plan-to-allow-employees-to-work-remotely-some-of-the-time

[3] Estimated by telecommunications trade association GSMA; https://www.gsma.com/iot/wp-content/uploads/2018/08/GSMA-IoT-Infographic-2019.pdf The International Data Corporation forecast 42.6 billion connected machines, sensors, and cameras; https://www.idc.com/getdoc.jsp?containerId=prUS45213219.

[4] World Economic Forum, Global Risks Report 2020. http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf

[5] European Union Agency for Cybersecurity (ENISA). (2020). *Main Incidents in the EU and worldwide.* ENISA. Retrieved from https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/etl-review-folder/etl-2020-main-incidents

[6] **The European Union Agency for Cybersecurity, ENISA**, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. https://www.enisa.europa.eu/about-enisa

Cyber risks have emerged as a significant threat to the financial system as well. The International Monetary Fund has estimated the annual loss due to cyber-attacks at 9% of banks' net income globally, or **around $100 billion**.[7]

According to the European Commission the impact on European businesses and organisations of a specific type of cyber incident, namely cyber theft of trade secrets the estimated cost for cyber theft of trade secrets is **the astonishing €60 billion** in economic growth and up to 289,000 jobs in the EU. [8]

Moreover, cybersecurity is intrinsically a global threat. According to the World Economic Forum Cyberattacks is one of the most likely global risks. Cyberattacks have become a common hazard for individuals and businesses rank them as the **seventh most likely and eighth most impactful risk, and the second most concerning risk for doing business globally** over the next 10 years. [9]

The figures show that exists an increasing danger posed by cybercriminals activities which obliges the **EU to take strong and urgent actions to protect the digital market and consequently our entire economy with a global and systemic approach.**

The EU is aware of these risks, not only with respect to the direct potential damages but also with **the loss of trust in the digital market**, which could lead to more serious repercussions. Without trust and security is impossible to develop or take advantage of the opportunities of the new digital age. Concerns about security are a major disincentive to using online services.[10] Around two-fifths of EU users have experienced security-related problems and three-fifths feel unable to protect themselves against cybercrime. [11]

Concrete steps have been taken by European Union with different policies, namely, the EU Cybersecurity Strategies, Network and Information Security Directive (NISD), the EU Cybersecurity Act or with the adoption of the General Data Protection Regulation (GDPR), which reflect the current regulatory strategy on data protection, critical infrastructure against cybersecurity risks.

---

[7] Lagarde, C. (22 june 2018). *https://blogs.imf.org/2018/06/22/estimating-cyber-risk-for-the-financial-sector/*. Retrieved from https://blogs.imf.org/2018/06/22/estimating-cyber-risk-for-the-financial-sector/

[8] PricewaterhouseCoopers and European Commission. (2019). *The scale and impact of industrial espionage and theft of trade secrets through cyber.* Brussels: EUROPEAN COMMISSION. Retrieved from https://op.europa.eu/en/publication-detail/-/publication/b3b5fcfb-4541-11e9-a8ed-01aa75ed71a1/language-en/format-PDF/source-search

[9] World Economic Forum. (2020). *Global Risks Report.* Retrieved from http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf

[10] https://data.europa.eu/euodp/en/data/dataset/S2249_92_2_499_ENG

[11] 2020 Digital Economy and Society Index; https://ec.europa.eu/digital-single-market/en/news/digital-economy-and-society-index-desi-2020; https://data.europa.eu/euodp/en/data/dataset/S2249_92_2_499_ENG

Considering the above context cybersecurity deserves a serious reflection about the EU and in particular the digital market functioning. **Concerns about security are a major disincentive to using online services.** The risk of **the loss of trust in the digital market** could generate serious repercussions on business, so cybersecurity appears the enabler of trust in emerging use cases for digital services and thus it can facilitate the transformation.

This is not only a business issue that justifies this paper, but also, as we have mentioned, *"the EU's economy, democracy and society depend more than ever on secure and reliable digital tools and connectivity."*

As stated in the new cybersecurity strategy: *"Improving cybersecurity is therefore essential for people to trust, use, and benefit from innovation, connectivity and automation, and for safeguarding fundamental rights and freedoms, including the rights to privacy and to the protection of personal data, and the freedom of expression and information."* [12]

Considering the above context, the following paperwork is dedicated in its first section to present an overview of cybersecurity, with abroad definition of cybersecurity. The purpose is to offer a basic understanding of the concept used in the EU cybersecurity strategy and regulations treated in this paper.

The second section is dedicated to the study of cybersecurity strategy policy and regulation of the European Union. We started with an introduction paragraph, regarding the complexity of the European cybersecurity scenario. It will describe the efforts of the EU institutions to build a strong cyber resilience which needs a collective and wide-ranging approach due to the **complexity and multi-layered setting.**

Moreover, it is going to compare how the regulations address security and privacy requirements, where principles and objectives are implemented by technological tools and organizational procedures, illustrating the differences and highlighting the areas of overlap among them in areas such as mitigation measures (data breaches), risk approach, notification obligations.

The last section is dedicated to present some conclusions, that sum up the most important insights of the paper and includes some recommendations for the EU authorities to fill the possible gaps in his cybersecurity strategy.

[12] EUROPEAN COMMISSION. (16 december 2020). JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL The EU's Cybersecurity Strategy for the Digital Decade. Brussels. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020JC0018&from=ga

I. What is cybersecurity?

As stated by ENISA in the paper "*Definition of Cybersecurity Gaps and overlaps in standardisation"* it is not easy to define what is cybersecurity: *"The problem is that* ***Cybersecurity is an enveloping term,*** *and it is not possible to make a definition to cover the extent of the things Cybersecurity covers."*[13]

It is extremely complicated to develop a cybersecurity definition which can encompass of information technology field and the **enormity of cyberspace**. [14]

As explained in the mentioned paper, ***"even the correct spelling of 'Cybersecurity' is controversial and differing.*** *Some publications use a single word 'Cybersecurity', others prefer a term consisting of two words 'Cyber Security'* [15]

In the light of the above considerations, it can sum up all the elements in the following definition:

"Cybersecurity shall refer ***to security of cyberspace****, where cyberspace itself refers to the set of links and relationships between objects that are accessible through a generalised telecommunications network, and to the set of objects themselves where they present interfaces allowing their remote control, remote access to data, or their participation in control actions within that Cyberspace.* ***Cybersecurity shall therefore encompass the CIA paradigm[16]*** *for relationships and objects within cyberspace and extend that same CIA paradigm to address protection of privacy for legal entities (people and corporations), and to address resilience (recovery from attack)."* [17]

This definition proposed by ENISA using ***"a contextual definition"*** **because cybersecurity is a broad and evolving term,** arguing that whereas opting for a specific definition can allow for maintaining clarity,

---

[13] European Union Agency for Cybersecurity (ENISA). (01 july 2015). *Definition of Cybersecurity - Gaps and overlaps in standardisation.* Heraklion, Greece: ENISA. doi:DOI 10.2824/4069

[14] "*Information technology involving the development, maintenance, and use of computer systems, software, and networks for the processing and distribution of data".* Merriam-Webster. (n.d.). Information technology. In Merriam-Webster.com dictionary. Retrieved from https://www.merriam-webster.com/dictionary/information%20technology . Clearly, this definition includes four fundamental elements that shape the Information Technology system: 1. Computer (in other words, Hardware) 2. Software 3. Networks and, 4. Data.

[15] European Union Agency for Cybersecurity (ENISA). (01 July 2015). *Definition of Cybersecurity - Gaps and overlaps in standardisation.* Heraklion, Greece: ENISA. doi:DOI 10.2824/4069

[16] NOTE: In short, when we try to protect information the most common goals to achieve are **confidentiality, integrity and availability. These goals are commonly called 'CIA triad'** and, as we have seen previously, we can define in the following way: Confidentiality: prevent unauthorised information gain. Integrity: prevent or detect unauthorised modification of data. Availability: prevent unauthorised deletion or disruption.

[17] European Union Agency for Cybersecurity (ENISA). (01 July 2015). *Definition of Cybersecurity - Gaps and overlaps in standardisation.* Heraklion, Greece: ENISA. doi:DOI 10.2824/4069

stakeholders and policy makers should select **definitions that fit their particular needs in a specific context**.[18]

II. An overview on policy and legislative EU framework complexity

Cybersecurity is essential for people to trust, use, and benefit from innovation, connectivity and automation, and for safeguarding **fundamental rights and freedoms, including the rights to privacy** and to the protection of personal data, and the **freedom of expression and information.**[19]

However, most of the scholars and papers studying EU cybersecurity strategy highlight the difficulty of analysing the policy and legislative cybersecurity landscape. As stated in the Briefing Paper *"Challenges to effective EU cybersecurity policy"*:

"The EU's cyber ecosystem is complex and multi-layered, cuts across an array of internal policy areas, like justice and home affairs, the digital single market and research policies**. In external policy, cybersecurity features in diplomacy, and is increasingly part of the EU's emerging defence policy…involving many stakeholders. **Bringing together all of its disparate parts is a considerable challenge." [20]

The legislative and policy landscape is complex, due to the elevated number of policies and legislative regulations, which need to be periodically amended considering the technological advances. The following table shows the timeline of the most important:

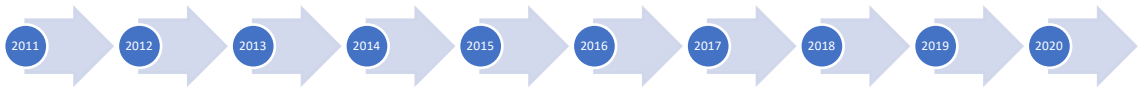
[18] *Idem.*

[19] EUROPEAN COMMISSION. (16 December 2020). JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL The EU's Cybersecurity Strategy for the Digital Decade. Brussels. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020JC0018&from=ga

[20] EUROPEAN COURT OF AUDITORS. "Challenges to effective EU cybersecurity policy." 2019. https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_EN.pdf

Table 1.: Timeline of the most important cybersecurity policies and legislation

Policy									
Legislation									
e-Privacy Directive (e-Privacy Directive 2: 2021)	CERT-EU	Directive on attacks on Information systems	EIDAS	PSD 2	NISD (NISD2: 2021)	Building strong cybersecurity for the EU Identification	GDPR	EU Cyber-security Act	Cybersecurity Competence Centre
		EU Cyber-security strategy	EU Cyber Defence Policy (updated 2018)						New EU's Cybersecurity Strategy



Source: Own elaboration

Considering this complex scenario, it seems necessary to reduce the focus on the most important policy and legislatives acts. With this in mind, in the following chapter it will be analysed the most relevant strategic acts in the cybersecurity EU field.

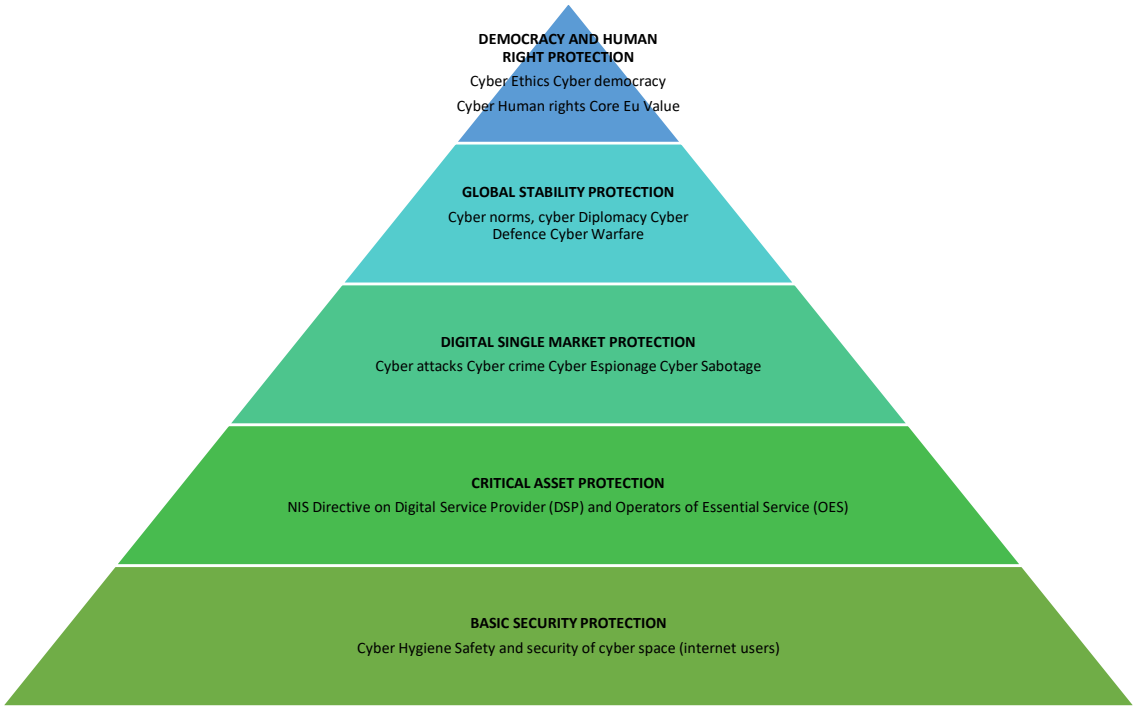
3.1. The cybersecurity strategy of the European Union

In the 2013 the European Union institutions published jointly what we can considered the cornerstone of the EU cybersecurity strategy.[21] **The joint communication starts describing the context of the cyberspace in our daily live, highlighting the enormous benefits but also the vulnerabilities.**

Any EU strategy must cover all aspects of cyber space to ensure a comprehensive approach to addressing the cyber challenges. **This strategy clarifies the principles that should guide cybersecurity policy in the EU and internationally to protect the needs, values and humans' rights.**

[21] EUROPEAN COMMISSION. (07 February 2013). JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS. *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*. Brussels. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52013JC0001&from=EN

Figure 1.: Layers of cybersecurity protection



Own elaboration based on: ENISA (2017). Overview of cybersecurity and related terminology

Figure 1. presents ENISA's perspective on cyber space needs, starting with EU core values, such as democracy and human rights at the top, and, working the way down, to the basic citizens' needs.

After seven years from the publication of the first strategy, the EU has considered necessary to make another step to build up a more stringent and robust strategy, publishing a **new strategy act.**

As stated in the first paragraph of the new strategy, "***cybersecurity is an integral part of Europeans' security.*** *Whether it is connected devices, electricity grids, or banks, aircraft, public administrations or hospitals they use or frequent, people deserve to do so within the assurance that they will be shielded from cyber threats. The EU's economy, democracy and society depend more than ever on secure and reliable digital tools and connectivity.* ***Cybersecurity is therefore essential for building a resilient, green and digital Europe."*** [22]

Following the progress achieved under the previous strategies, it contains concrete proposals for deploying three principal instruments –regulatory, investment and policy instruments – to address **three areas of EU action:**

[22] EUROPEAN COMMISSION. (16 December 2020). JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL The EU's Cybersecurity Strategy for the Digital Decade. Brussels. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020JC0018&from=ga

1. resilience, technological sovereignty and leadership,
2. building operational capacity to prevent, deter and respond, and
3. advancing a global and open cyberspace.

3.2. EU Cybersecurity Act

European Union is aware of the need for a strong and reliable cybersecurity strategy. For this reason, in 2019 the EU published a new regulation called: Cybersecurity Act.[23]

The first objective of the regulation is to establish **a certification scheme about the cybersecurity features of ICT products, ICT services and ICT processes to tackle the current fragmentation of the internal market.** To achieve this object the article 1 sets out that the European Union Agency for Network and Information Security (ENISA) will play a decisive role in the certification process.

In fact, as on many occasions highlighted by the EU institutions, the lack of interoperable solutions (technical standards), practices and Union-wide mechanisms of certification are among the other gaps affecting the single market in the field of cybersecurity. *"This makes it difficult for European businesses to compete at national, Union and global level. It also reduces the choice of viable and usable cybersecurity technologies that individuals and businesses have access to."*[24]

Also, it is very important that the European **cybersecurity certification framework** should be established in a uniform manner in all Member States in order to prevent 'certification shopping' based on different levels of stringency in different Member States.

The purpose of European cybersecurity certification schemes should be to ensure that ICT products, ICT services and ICT processes certified under such **schemes comply with specified requirements that aim to protect the availability, authenticity, integrity and confidentiality of stored, transmitted or processed data** or of the related functions of or services offered by, or accessible via those products, services and processes throughout their life cycle.

---

[23] EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION. (17 April 2019). REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 April 2019. *on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)*. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN

[24] EUROPEAN COURT OF AUDITORS. (2019). *Challenges to effective EU cybersecurity policy.* European Union. Retrieved from https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_EN.pdf

3.3. NIS Directive and its next reform

The DIRECTIVE (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (NIS) [25] is the first legal act to achieve the strategic priority **'Achieving Cyber resilience' set out in the Cybersecurity Strategy of the EU.**

As mentioned above, the first Cybersecurity Strategy of the EU includes several fundamental principles underlying the EU approach to cybersecurity followed by 5 strategic priorities. *"The proposal for the NIS Directive was thus made under the first strategic priority 'Achieving Cyber resilience'."* [26]

The NIS Directive highlights the *"lack of common requirements on operators of essential services and digital service providers",* stating that ***"Member States have very different levels of preparedness, which has led to fragmented approaches across the Union.*** *This results in an unequal level of protection of consumers and businesses and undermines the overall level of security of network and information systems within the Union."*

In this context of fragmentation, the purpose of the directive is to achieve *"a high common level of security of networks and information systems within the Union* ***so as to improve the functioning of the internal market."***

The aim of the NIS Directive is to establish a common level of security for network and information systems, since these systems are a vital component to address the risks that may be posed in important sectors of a society. The NIS Directive focuses on two types of service providers, the Operators of Essential Services ("OES") and the relevant Digital Service Providers ("DSPs").[27]

The main points of the **NIS Directive** can be summarised as follows:

[25] EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION. (06 de july de 2016). DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016 concerning measures for a high common level of security of network and information systems. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN

[26] European Union Agency for Cybersecurity (ENISA). (2017). *Incident notification for DSPs in the context of the NIS Directive.* ENISA. Retrieved from https://www.enisa.europa.eu/publications/incident-notification-for-dsps-in-the-context-of-the-nis-directive/at_download/fullReport

[27] Cyberwatching Consortium. (2019). *Cybersecurity legal and policy aspects: preliminary recommandations and road ahead.* Cyberwatching.

Table 2.: Main points of the NIS Directive

MAIN POINTS	ACTIONS FOR THE MEMBER STATES
Improved cybersecurity capabilities at national level:	Adopt a national strategy on the security of network and information systems defining the strategic objectives and appropriate policy and regulatory measures. Designate one or more national competent authorities for the NIS Directive and a national single point of contact, to monitor the application of the Directive at national level. Designate one or more Computer Security Incident Response Teams (CSIRTs) for comprehensive incident management nationwide.
Increased EU-level cooperation:	Establishes an EU level Cooperation Group, to support and facilitate strategic cooperation and the exchange of information among Member States and to develop trust and confidence. Establishes an EU level network of the national CSIRTs and CERT-EU, in order to contribute to the development of confidence and trust between the Member States and to promote swift and effective operational cooperation. ENISA will provide the secretariat of the group.
Security measures and incident reporting obligations for operators of essential services and digital service providers:	Identified operators of essential services (OESs) and digital service providers (DSPs) will have to take appropriate security measures and to notify serious incidents to the relevant national authority.

Source: Own elaboration

The first EU-wide law on cybersecurity, the NIS Directive, came into force in 2016 and helped achieve a higher and more even level of security of network and information systems across the EU. In view of the unprecedented digitalisation in the last years, the time has come to refresh it.[28]

The Commission proposal expands the scope of the current NIS Directive by adding new sectors based on their how crucial they are for the economy and society, and by introducing a clear size cap – meaning that all medium and large companies in selected sectors will be included in the scope. At the same time, it leaves some flexibility for Member States to identify smaller entities with a high security risk profile.[29]

The proposal also eliminates the distinction between operators of essential services and digital service providers. Entities would be classified based on their importance, and divided into essential and important categories, which will be subjected to different supervisory regimes.[30]

The proposal strengthens and streamlines security and reporting requirements for companies by imposing a risk management approach, which provides a minimum list of basic security elements that have to be applied. The proposal introduces more precise provisions on the process for incident reporting, content of the reports and timelines.

The proposal introduces more stringent supervisory measures for national authorities, stricter enforcement requirements and aims at harmonising sanctions regimes across Member States.

The proposal also enhances the role of the Cooperation Group in shaping strategic policy decisions and increases information sharing and cooperation between Member State authorities. It also enhances operational cooperation including on cyber crisis management.

The Commission proposal also establishes a basic framework with responsible key actors on coordinated vulnerability disclosure for newly discovered vulnerabilities across the EU and creates EU registry in this area, operated by ENISA.

[28] EUROPEAN COMMISSION (2020) DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=72166

[29] https://ec.europa.eu/digital-single-market/en/news/proposal-directive-measures-high-common-level-cybersecurity-across-union

[30] https://ec.europa.eu/digital-single-market/en/faq/faq-revision-network-and-information-security-directive

Table 3.: How change the NIS directive

NIS	NIS 2			
	GREATER CAPABILITIES			
EU Member States improve their cybersecurity capabilities	More stringent supervision measures and enforcement are introduced	A list of administrative sanctions, including fines for breaches of the cybersecurity risk management and reporting obligations is established		
	COOPERATION			
Increased EU-Level	Establishment of European cyber crises laison organisation network (EU-CyCLONe) to support coordinated management of large-scale cybersecurity incidents and crises at EU level	Increased information sharing and cooperation between Member State authorities with enhanced role of the Cooperation group.		Coordinated vulnerability disclosure for newly discovered vulnerabilities across the EU is established
	CYBERSECURITY RISK MANAGEMENT			
Operators of Essential Services (OES) and Digital Service Providers (DSP) have to adopt risk management practices and notify significant incident to their national authorities	Strengthened security requirements with a list of focused measures including incident response and crisis management, vulnerability handling and disclosure, cybersecurity testing and the effective use of encryption.	Cybersecurity of supply chain for key information and communication technologies will be strengthened.	Accountability of the company management for compliance with cybersecurity risk management measures.	Streamlined incident reporting obligations with more precise provisions on the reporting process, content and timeline.

Source: Own elaboration based on: EUROPEAN COMMISSION. [31]

[31] https://ec.europa.eu/digital-single-market/en/news/revised-directive-security-network-and-information-systems-nis2

3.4. GDPR: General Data Protection Regulation

The General Data Protection Regulation (EU) 679/20161 ('GDPR') will be, as of 25 May 2018, the main data protection legal framework in EU directly applicable to all Member States, repealing the current Data Protection Directive 95/46/EC2. Under the Regulation, one of the core obligations for all businesses, acting either as data controllers or data processors, is that of the security of personal data processing.[32]

The relevance of the protection in personal data is stated from the first line of the Regulation, where says that: ***"the protection of natural persons in relation to the processing of personal data is a fundamental right.*** *Article 8(1) of the Charter of Fundamental Rights of the European Union (the 'Charter') and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) provide that everyone has the right to the protection of personal data concerning him or her."*[33]

The regulation is aware that: *"Rapid technological developments and globalisation have brought* ***new challenges for the protection of personal data.*** *The scale of the collection and sharing of personal data has increased significantly. Technology allows both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities. Natural persons increasingly make personal information available publicly and globally."* [34]

The principles of data protection should apply to any information concerning an **identified or identifiable natural person.** Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them. [35]

On the one side, the GDPR's obligations are represented by the overarching principle of accountability, which is established in Art. 5(2) GDPR. The principle of accountability states that controllers are responsible for complying with the GDPR requirements (mainly spelled out in terms of principles in Art. 5(1)):

---

[32] EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION. (27 April 2016). REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016. *on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

[33] *Idem.*

[34] *Idem.*

[35] European Union Agency for Cybersecurity (ENISA). (12 January 2015). Privacy and Data Protection by Design. Retrieved from https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design/at_download/fullReport

- lawfulness, fairness and transparency.
- purpose limitation.
- data minimisation.
- accuracy.
- storage limitation; and
- integrity and confidentiality, as well as for being able to demonstrate their compliance, in a manner which can be understood.

An integral part of the principle of accountability is the so-called **"risk-based approach".** According to GDPR security equally covers confidentiality, integrity and availability and should be considered following a risk-based approach: **the higher the risk, the more rigorous the measures that the controller or the processor needs to take (in order to manage the risk).**

Even if this **risk-based approach** is not a new concept only a few specific privacy risk assessment frameworks have been presented, focusing principally on the evaluation of risks to personal data and adoption of relevant security measures.[36]

In particular, the security of personal data processing is mainly mandated in crucial **Article 32 of GDPR,** which states that:

'Having regard to the state of the art and the costs of implementation and taking into account the nature, scope, context and purposes of the processing as well as the risk of varying likelihood and severity for the rights and freedoms of individuals, ***the controller and the processor shall implement appropriate technical and organisational measures,*** *to ensure a level of security appropriate to the risk, including inter alia, as appropriate:*

(a) the pseudonymisation and encryption of personal data.
(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of systems and services processing personal data.
(c) the ability to restore the availability and access to data in a timely manner in the event of a physical or technical incident.
(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.'

[36] European Union Agency for Cybersecurity (ENISA). (2018). *Handbook on Security of Personal Data Processing.* Retrieved from https://www.enisa.europa.eu/publications/handbook-on-security-of-personal-data-processing/at_download/fullReport

The article further stipulates that: *'in assessing the appropriate level of security account shall be taken in particular of the* ***risks that are presented by data processing,*** *in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed'. It also mentions that adherence to an approved code of conduct (Article 40 GDPR) or an* ***approved certification mechanism*** *(Article 41 GDPR) may be used as an element to demonstrate compliance with the requirements for the security of processing."*

Last, it states that the controller and processor: '*shall take steps to ensure that any person acting under their authority and having access to personal data, shall not process them except on instructions from the controller, unless otherwise required by Union or member state law'.*[37]

In this sense, standards such as **ISO 27001 encourage the adoption of a security standard organization structure**. This is largely due to the fact that these **organizational standards provide a blueprint for setting up a management system for security,** but also a blueprint for auditing and checking compliance of an organization to security best practices.[38]

This International Standard has been prepared by ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization to provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an **Information Security Management System (ISMS).** [39]

Recognizing the role of defaults in the protection of personal data, the General Data Protection Regulation (GDPR) provides under its Article 25 (2) a new obligation for data controllers with regard to **data protection by default.**

In particular, it mandates that the controller, by the use of appropriate technical and organisational measures, shall ensure that only personal data that are necessary for the purpose are processed. This is applicable to the amount of the personal data collected, the extent of their processing, the period of storage and their accessibility. Moreover, the controller shall ensure that by default personal data are not made accessible, without the individual's intervention, to an indefinite number of natural persons.

---

[37] *idem*

[38] Purser, S. (2011). *Standards for cyber security. Euroepan Network and information Security Agency (ENISA).* Retrieved from https://www.enisa.europa.eu/publications/articles/standards-for-cyber-security

[39] ISO (International Organization for Standardization) and IEC (the International Electrotechnical Commission) . (2005). *Information technology — Security techniques — Information security management systems — Requirements INTERNATIONAL STANDARD ISO/IEC 27001 Fir.*

The obligation for data protection by default is closely interlinked with the one on **data protection by design** stipulated in Article 25(1) GDPR, which states that "*the controller shall implement appropriate technical and organisational* ***measures designed to implement the data protection principles of GDPR*** *in an effective manner and integrate the necessary safeguards into the processing of personal data.* ***In fact, data protection by default could be seen as a natural extension of data protection by design*** *when it comes to choosing the data protection friendly default settings."*

Together, data protection by design and by default, fall within the overall notion of privacy engineering, i.e., embedding privacy requirements into the information systems' design and operation. In this way, **data protection by design and by default, are also closely interlinked with security of processing (article 32 GDPR),** which is another essential GDPR requirement. [40]

V. Conclusions

The information collected and processed for this paper has produced several interesting findings leading to some conclusions on cybersecurity strategy of European Union.

1) Cybersecurity is very relevant due to the impact on fundamental rights.

The first conclusion is inferred from the first lines of this paper. **There is no doubt about the importance of cybersecurity**, considering the potential impact on the fundamental right to privacy and to the protection of personal data, and the freedom of expression and information. In the words of EU:

"*Improving cybersecurity is therefore essential for people to trust, use, and benefit from innovation, connectivity and automation, and for* ***safeguarding fundamental rights and freedoms, including the rights to privacy and to the protection of personal data, and the freedom of expression and information."*** [41]

2) The study of cybersecurity faces some clear challenges.

However, a systematic study regarding cybersecurity faces some **challenges**:

[40] *Idem*

[41] EUROPEAN COMMISSION. (16 December 2020). JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL The EU's Cybersecurity Strategy for the Digital Decade. Brussels. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020JC0018&from=ga

The first challenge has been to demonstrate the **complexity of the cybersecurity scenario, due to the enormity of cyberspace.** From the apparently simple task of definition, the difficulty to find a coherent and precise area of study arises.

The second is that cybersecurity is **inherently multidisciplinary, a complex subject that requires knowledge and expertise from multiple disciplines:** information technology, political science, engineering, economics and law, among others.

Finally, **cybersecurity is a global and multi-national** fast-moving nature issue with cyber-attacks are rarely restricted to a sole jurisdiction.

To summarise, the approach at any specific cybersecurity study must consider, for instance, **the sector, the applications and technology, research domains and eventually the global complexity and multi-layered aspect of cybersecurity.**

3) Cybersecurity is basically a technological issue, but the human factor is fundamental.

Despite the difficulty to study cybersecurity, this study puts the focus on the essential features of cybersecurity, mentioning what is generally called the ***"triad of cybersecurity"*** **(CIA)** in cybersecurity areas: **Confidentiality, Integrity and Availability,** keeping in mind the difference between a) the defence of network and infrastructure and b) the information stored or transmitted by this network and infrastructure.

Actually, the NIS Directive includes the CIA concept in his art. 4.2. when defining cybersecurity as: "*the ability of network and information systems to resist, at a given level of confidence, any action that compromises the* ***availability, authenticity, integrity or confidentiality of stored or transmitted or processed data*** *or the related services offered by, or accessible via, those network and information systems".*

This definition is in line with the EU Cybersecurity Strategy as well, where cybersecurity is considered as ***"the availability and integrity of the networks and infrastructure and the confidentiality of the information contained therein".***

In order to ensure the availability, integrity and confidentiality, there are technologies, for instance, **encryption technology**, which are currently the most important tool to ensure a digitally secure environment. These technologies represent the most important instruments mentioned in the different regulations in order to protect information.

Nevertheless, **the most sophisticated technology can be useless or worst dangerous if the users are not able to understand these technological tools**, for instance, a weak password configuration.

4) The use of standards in cybersecurity is key.

The importance of the standards and certifications in order to harmonize the implementation of technical and organizational cybersecurity measures cannot be undermine, **because there is no doubt that the implementation of standards in cybersecurity field can be an adequate solution to achieve compliance with the regulations, ensure the harmonization regulation in the EU and enhance security requirements.**

As a matter of fact, cybersecurity faces the same problem present in many other fields in the EU policy, that is mean, **the lack of harmonization which leads to a fragmented approach across the Union,** due to the need for a vertical consistency at the level of both the EU and Member States.

In this sense, Member States have very different levels of preparedness, which has led to fragmented approaches across the Union. This results in an unequal level of protection of consumers and businesses and undermines the overall level of security of network and information systems within the Union. Lack of common requirements on operators of essential services and digital service providers in turn makes it impossible to set up a global and effective mechanism for cooperation at Union level.[42]

As suggested by Ramses Wessel, cybersecurity forms *"an excellent example of an area in which the different policy fields need to be combined* ***(a requirement for horizontal consistency),*** *and where measures need to be taken at the level of both the EU and Member States* ***(calling for vertical consistency)".*** [43]

5) European Union plays a crucial role in cybersecurity.

European's action seems to be necessary and proportional considering **the supranational nature of cybersecurity attacks**, and in line with the principle of conferral the protection cannot be sufficiently achieved by the Member States, either at central level or at regional and local level and whereas can be better achieved at Union level.

---

[42] Dominik Herrmann and Pridöhl Henning. (2020). Basic Concepts and Models of Cybersecurity. En M. C. Loi (Ed.), *The Ethics of Cybersecurity* (págs. 11-44). Springer Open. doi:10.1007/978-3-030-29053-5_2

[43] Wessel RA (2015) Towards EU cybersecurity law: regulating a new policy field. In: Tsagourias N, Buchan R (eds) Research handbook on international law and cyberspace. Edward Elgar Publishing. Text extracted from Dominik Herrmann and Pridöhl Henning. (2020). Basic Concepts and Models of Cybersecurity. En M. C. Loi (Ed.), *The Ethics of Cybersecurity* (pág. 98). Springer Open. doi:10.1007/978-3-030-29053-5_2. (Chapter 5 Cybersecurity Regulation in the European Union: The Digital, the Critical and Fundamental Rights Gloria González Fuster and Lina Jasmontaite)

However, the application of **Non-European international standards,** such as NIST or ISO standards, cannot be the most appropriate response because these standards do not take in account the singularity and interest of European market.

As a matter of fact, the last efforts of the EU are being made in the field of promoting a **Single Market for Cybersecurity harmonization regarding products and services in order to implement a uniform European cybersecurity certification and standard,** a common ground for all member states.

In this sense, the Cybersecurity strategy underlines the importance of the ETSI, CEN CENELEC and ENISA, by stating: *"the Commission will support the **development of security standards**"; "Such work should build on the on-going standardisation work of the European Standardisation Organisations (CEN, CENELEC and ETSI), of the Cybersecurity Coordination Group (CSCG) as well as on the expertise of ENISA, the Commission and other relevant players".*

We need to keep in mind that in the absence of EU initiatives and leadership in this area there is a growing risk of de facto standardisation of practices via market consolidation as innovative EU-based service providers may gradually be consolidated in **non-EU-led groups of companies**.[44]

The creation of EU cybersecurity standard and certification will: *"**Support the development of an EU cybersecurity industry ("made in Europe")** […] to enhance the security of digital systems and **guarantee the fundamental rights of EU citizens, while also increasing job creation and European competitiveness in the global market."*** [45]

Moreover, EU can enhance further coordination and cooperation between EU actors, as well as with and between Member States. For instance, with a Joint Cyber Unit would serve as a virtual and **physical platform for cooperation for the different cybersecurity communities in the EU to foster the cooperation and exchange between cybersecurity actors and law enforcement.**

But, if there are rooms for improvements, the study also has revealed that **extraordinary work done by the EU institutions in this last decade**, developing common rules, proposing new regulations: NIS Directive and the Cybersecurity Act, creating new institutions: ENISA, with the purpose to build a strong and secure digital environment.

[44] European Union Agency for Cybersecurity (ENISA). (2019). *Guidance and gaps analysis for European standardisation.* Retrieved from https://www.enisa.europa.eu/publications/guidance-and-gaps-analysis-for-european-standardisation/at_download/fullReport

[45] European Commission. (2017). *Cybersecurity in the European Digital Single Market.* High Level Group of Scientific Advisors . Brussels: Scientific Advice Mechanism (SAM). Retrieved from https://op.europa.eu/s/o9Rv

6) There are cybersecurity paradigms shared across the regulations.

The analysis of some of the main compulsory mechanisms of the legal framework on cybersecurity has allowed **identifying the key elements of the various legal provisions critical to data security and cybersecurity strategy,** revealing the interconnections between the different legal instruments. This core element should be considered as a baseline security requirement which can then be transposed to widely accepted technical specifications, certifications and standards.

Key References and Useful links

2020 Digital Economy and Society Index; https://ec.europa.eu/digital-single-market/en/news/digital-economy-and-society-index-desi-2020; https://data.europa.eu/euodp/en/data/dataset/S2249_92_2_499_ENG

Cyberwatching Consortium. (2019). *Cybersecurity legal and policy aspects: preliminary recommandations and road ahead.* Cyberwatching.

Dominik Herrmann and Pridöhl Henning. (2020). Basic Concepts and Models of Cybersecurity. En M. C. Loi (Ed.), *The Ethics of Cybersecurity* (págs. 11-44). Springer Open. doi:10.1007/978-3-030-29053-5_2

Estimated by telecommunications trade association GSMA; https://www.gsma.com/iot/wp-content/uploads/2018/08/GSMA-IoT-Infographic-2019.pdf The International Data Corporation forecast 42.6 billion connected machines, sensors, and cameras; https://www.idc.com/getdoc.jsp?containerId=prUS45213219.

EUROPEAN COMMISSION (2020) DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=72166

EUROPEAN COMMISSION. (07 February 2013). JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS. *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*. Brussels. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52013JC0001&from=EN

EUROPEAN COMMISSION. (16 december 2020). JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL The EU's Cybersecurity Strategy for the Digital Decade. Brussels. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020JC0018&from=ga

European Commission. (2017). *Cybersecurity in the European Digital Single Market.* High Level Group of Scientific Advisors . Brussels: Scientific Advice Mechanism (SAM). Retrieved from https://op.europa.eu/s/o9Rv

European Commission. (2020). *Telework in the EU before and after the COVID-19: where we were, where we head to.* Retrieved from https://ec.europa.eu/jrc/sites/jrcsh/files/jrc120945_policy_brief_-_covid_and_telework_final.pdf

EUROPEAN COURT OF AUDITORS. (2019). *Challenges to effective EU cybersecurity policy.* European Union. Retrieved from https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_EN.pdf

EUROPEAN COURT OF AUDITORS. “Challenges to effective EU cybersecurity policy.” 2019. https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_EN.pdf

EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION. (06 de july de 2016). DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016 concerning measures for a high common level of security of network and information systems. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN
EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION. (17 April 2019). REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 April 2019. *on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)*. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN

European Union Agency for Cybersecurity (ENISA). (01 July 2015). *Definition of Cybersecurity - Gaps and overlaps in standardisation.* Heraklion, Greece: ENISA. doi:DOI 10.2824/4069

European Union Agency for Cybersecurity (ENISA). (12 January 2015). Privacy and Data Protection by Design. Retrieved from https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design/at_download/fullReport

European Union Agency for Cybersecurity (ENISA). (2017). *Incident notification for DSPs in the context of the NIS Directive.* ENISA. Retrieved from https://www.enisa.europa.eu/publications/incident-notification-for-dsps-in-the-context-of-the-nis-directive/at_download/fullReport

European Union Agency for Cybersecurity (ENISA). (2018). *Handbook on Security of Personal Data Processing.* Retrieved from https://www.enisa.europa.eu/publications/handbook-on-security-of-personal-data-processing/at_download/fullReport

European Union Agency for Cybersecurity (ENISA). (2019). *Guidance and gaps analysis for European standardisation.* Retrieved from https://www.enisa.europa.eu/publications/guidance-and-gaps-analysis-for-european-standardisation/at_download/fullReport

European Union Agency for Cybersecurity (ENISA). (2020). *Main Incidents in the EU and worldwide.* ENISA. Retrieved from https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/etl-review-folder/etl-2020-main-incidents

Gartner. (14 July 2020). *Gartner Survey Reveals 82% of Company Leaders Plan to Allow Employees to Work Remotely Some of the Time*. Retrieved from https://www.gartner.com/en/newsroom/press-releases/2020-07-14-gartner-survey-reveals-82-percent-of-company-leaders-plan-to-allow-employees-to-work-remotely-some-of-the-time

ISO (International Organization for Standardization) and IEC (the International Electrotechnical Commission) . (2005). *Information technology — Security techniques — Information security management systems — Requirements INTERNATIONAL STANDARD ISO/IEC 27001 Fir.*

Lagarde, C. (22 june 2018). *https://blogs.imf.org/2018/06/22/estimating-cyber-risk-for-the-financial-sector/*. Retrieved from https://blogs.imf.org/2018/06/22/estimating-cyber-risk-for-the-financial-sector/

PricewaterhouseCoopers and European Commission. (2019). *The scale and impact of industrial espionage and theft of trade secrets through cyber.* Brussels: EUROPEAN COMMISSION. Retrieved from https://op.europa.eu/en/publication-detail/-/publication/b3b5fcfb-4541-11e9-a8ed-01aa75ed71a1/language-en/format-PDF/source-search

Purser, S. (2011). *Standards for cyber security. Euroepan Network and information Security Agency (ENISA).* Retrieved from https://www.enisa.europa.eu/publications/articles/standards-for-cyber-security

Wessel RA (2015) Towards EU cybersecurity law: regulating a new policy field. In: Tsagourias N, Buchan R (eds) Research handbook on international law and cyberspace. Edward Elgar Publishing. Text extracted from Dominik

Herrmann and Pridöhl Henning. (2020). Basic Concepts and Models of Cybersecurity. En M. C. Loi (Ed.), *The Ethics of Cybersecurity* (pág. 98). Springer Open. doi:10.1007/978-3-030-29053-5_2. (Chapter 5 Cybersecurity Regulation in the European Union: The Digital, the Critical and Fundamental Rights Gloria González Fuster and Lina Jasmontaite)

World Economic Forum, Global Risks Report 2020.
http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf

With the support of the
Erasmus+ Programme
of the European Union