Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/CLSR

Computer Law & Security Review

Cybersecurity as *praxis* and as a *state*: The EU law path towards acknowledgement of a new right to cybersecurity?

Vagelis Papakonstantinou

Professor of Law, Faculty of Law and Criminology, Vrije Universiteit Brussel, Pleinlaan 2, 1050, Brussels, Belgium

A B S T R A C T

The end of the second decade of the 21st century has been the best of times for EU's cybersecurity law and policy: Its NIS Directive has been transposed into all Member States' national law, creating a new administrative structure at EU and Member State level and mandating relevant policies and strategies to update and harmonise those that were already in place. Its Cybersecurity Act of 2019 incorporated the EU Agency for Cybersecurity (ENISA), and promises to install a new European cybersecurity certification scheme. To support policy with funding, large sums of research money have been spent on the development of cybersecurity tools and the relevant framework. However, EU's significant regulatory activity is faced with substantial difficulties. While cybersecurity concerns are placed high on the list of issues that worry Europeans making a regulatory response pressing, the cybersecurity theoretical framework is far from concluded: Difficulties start as early as when attempting to define the term, ultimately divulging a lack of common understanding. Different actors understand cybersecurity differently under different circumstances. A distinction that could perhaps prove useful in creating clarity as to its exact meaning would distinguish between cybersecurity as *praxis* and cybersecurity as a *state*. Cybersecurity as *praxis* would then be understood as the activities and measures that need to be undertaken in order to accomplish cybersecurity's aims and objectives. Accordingly, cybersecurity as a *state* would mean the condition that is achieved once cybersecurity as *praxis* has succeeded; Within cybersecurity as a *state* persons need to be protected against any cyber threat. A distinction between cybersecurity as *praxis* and cybersecurity as a *state* would not only be useful in delineating the term's content but could also constitute the necessary theoretical groundwork for development, ultimately, of a new right to cybersecurity. EU law has already taken positive steps towards acknowledgement of a new right to cybersecurity. However, a lot more needs to be done; Past progress needs to be continued and updated. A conceivable next step could take the form of formal acknowledgement of such a new right in EU law, in a future amendment of the Act's provisions or otherwise.

1. Introduction

The end of the second decade of the 21st century has been the best of times for EU's cybersecurity law and policy: its NIS Directive[1] of 2016 has been transposed into all Member States' national laws,[2] creating a new administrative structure at EU and Member State level and mandating relevant policies and strategies to update and harmonise those that were already in place. Its Cybersecurity Act of 2019[3] incorporated

E-mail address: evangelos.papakonstantinou@vub.be

[1] 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 across the Union (the "NIS Directive").

[2] Information on incorporation and harmonisation may be found at the relevant EU Commission's web-pages, at https://ec.europa.eu/digital-single-market/en/state-play-transposition-nis-directive..

[3] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019on ENISA (the European Union Agency for Cybersecurity) and on information and communications technol-

https://doi.org/10.1016/j.clsr.2022.105653

the EU Agency for Cybersecurity (ENISA),[4] thus warranting its future and expanding its mandate; at the same time the Act also promises to install a new European cybersecurity certification scheme.[5] To support policy with funding, large sums of research money have been spent on the development of cybersecurity tools and the relevant framework.[6]

However, EU's significant regulatory activity is faced with substantial difficulties. On the one hand, cybersecurity concerns are placed high in the list of issues that worry Europeans.[7] This makes regulatory response pressing. On the other hand, the cybersecurity theoretical framework is far from concluded. Difficulties start as early as when attempting to even define the term: the many contexts and approaches to cybersecurity as well as the fact that its origins are traced in literature rather than specialised documentation, make it impossible to reach a generally agreed upon definition. This has led to definitional approaches that vary considerably, from acknowledging the impossibility of the task and questioning the very need for a definition, to providing complex and comprehensive wording that is more akin to a concept than a single term.

Definitional difficulties ultimately divulge a lack of common understanding. Different actors understand cybersecurity differently under different circumstances. A distinction that could perhaps shed some new light and create clarity as to its exact meaning would distinguish between cybersecurity as *praxis* and cybersecurity as a *state*. Cybersecurity as *praxis* would then be understood as the activities and measures to accomplish cybersecurity's aims and objectives. It would include a requirement to act, to undertake concrete actions. Accordingly, cybersecurity as a *state* would mean the condition that is achieved once cybersecurity as *praxis* has succeeded; within cybersecurity as a *state* natural and legal persons need to be protected against any cyber threat. Within its protective sphere natural and legal persons need to be (cyber)secure, to have a claim to remain so and for others to respect their wish.

A distinction between cybersecurity as *praxis* and cybersecurity as a *state* would not only be useful in delineating the term's content but could also constitute the necessary theoretical groundwork for development, ultimately, of a new right to cybersecurity. A new right to cybersecurity would allow natural and legal persons to defend themselves against cyber threats. It would place obligations upon all other parties to respect it, and, if applicable, take concrete actions in this regard. If a *state* of cybersecurity is to be achieved in EU law, a new right to cybersecurity is the suitable legal tool to create and defend it.

EU law has already taken positive steps towards acknowledgement of a new right to cybersecurity. Definite progress towards this direction may be viewed if the texts and the approaches of the NIS Directive and the EU Cybersecurity Act are put to comparison. The latter, although in a cautious and minimalistic manner, has taken important steps and made significant contributions towards identifying the basic components of a new right: the cybersecurity addressees and recipients, as well as, its subject-matter and scope. However, a lot more needs to be done; past progress needs to be continued and updated. A conceivable next step could take the form of formal acknowledgement of such a new right in EU law, in a future amendment of the Act's provisions, or otherwise.

The analysis that follows expands on each of the aforementioned topics: section 1 attempts to shed some light on cybersecurity in order to enhance and deepen understanding. To this end, subsection 1.1 illustrates the definitional impasse and the problems it causes for the cybersecurity purposes; subsection 1.2 introduces cybersecurity as *praxis*, focusing on its addressees and recipients, subject-matter and scope; subsection 1.3 introduces cybersecurity as a *state*, a conceptual condition of a protective sphere in which natural and legal persons are protected against cyber threats; The same section examines the relationship between cybersecurity and security. Section 2 attempts to make the theoretical findings of section 1 concrete onto EU law's current approach to cybersecurity. To this end, subsection 2.1 examines the development of the EU cybersecurity law framework, particularly focusing to the important contributions made by the EU Cybersecurity Act. Subsection 2.2 asks for formal acknowledgement of a new right to cybersecurity in EU law. Finally, subsection 2.3 seeks guidance in the neighbouring field of EU personal data protection law, as a *model par excellence* for cybersecurity, that could prove useful while addressing the, basic, question of EU competence to act in this field.

2. In search of clarity: cybersecurity as *praxis* and cybersecurity as a *state*

This section aims at shedding some light into the concept of cybersecurity, admittedly from a legal point of view. It is suggested that this could be achieved through distinction between cybersecurity as *praxis*, whereby actions and measures undertaken by the cybersecurity addressees are meant, and cybersecurity as a *state*, whereby a conceptual protective sphere is created to the benefit of the cybersecurity recipients within which they are and remain (cyber)secure. This distinction is considered useful in order to create clarity and improve understanding in today's complex global environment that creates confusion. Such confusion becomes evident as early as when trying to provide cybersecurity with a commonly accepted definition. The distinction between cybersecurity as *praxis* and as a *state* is also critical while examining existence of a new right to cybersecurity, because it sheds light into its necessary component parts: under a *praxis* lens the cybersecurity's addressees, recipients, as well as, its subject-matter and

ogy cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).

[4] That succeeded ENISA as was known until its release (see Recital 17 and also Chapter II of the EU Cybersecurity Act).

[5] See Chapter III, EU Cybersecurity Act.

[6] See the relevant European Commission's webpages on EU-funded projects on Digital security, at https://ec.europa.eu/digital-single-market/en/programme-and-projects/project-factsheets-digital-security

[7] See, for example, European Commission, "Special Eurobarometer 464a Report, Europeans' attitudes towards cyber security", September 2017, as well as, European Commission, "Cybercrime: new survey shows Europeans feel better informed but remain concerned", press release, 29 January 2020.

protective scope become identifiable; under a *state* lens, the cybersecurity protected sphere for natural and legal persons emerges, that in fact forms the core of the right to cybersecurity.

2.1. *The definitional impasse for cybersecurity*

A generally agreed upon definition for cybersecurity seems today more elusive than ever. This is reflected not only in the numerous (and at times contradicting) definitions to be found in formal texts of various aims, contexts and statuses, but also in an increase in recent years of academic contributions that are aimed exactly at addressing this problem.[8] Nevertheless, in order to establish existence of a (nascent) right to cybersecurity in EU law definitional clarity is of the essence. A right requires a well-described content that remains at all times identifiable both by its recipients and by its addressees. An "enveloping term" or even acceptance that a definition for cybersecurity is not necessary threatens to blur its scope and objectives and to create confusion as to its exact particulars.

Dictionaries define "*cybersecurity*" as "*measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack*"[9] or "*things that are done to protect a person, organization, or country and their computer information against crime or attacks carried out using the internet*"[10] or "*the state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this*".[11] The above three definitions already illustrate a dichotomy between actions ("*measures*", "*things*") and a condition ("*the state of*"), that will be elaborated in detail in subsections 1.2 and 1.3. Accordingly, in the USA cybersecurity has been defined as "*the ability to protect or defend the use of cyberspace from cyber attacks*",[12] adding therefore also an "*ability*" to "*actions*" or a "*state*" – an important element that will also be discussed in subsection 1.3.

Encyclopaedias, however, place emphasis on "*protection*" *per se*. In Britannica there is no "*cybersecurity*" term; instead, only "*computer security*" is listed (and is recommended when typing in "*cybersecurity*"): "*the protection of computer systems and information from harm, theft, and unauthorized use*".[13] Similarly, Wikipedia considers "*cybersecurity*", "*computer security*" and "*information technology security*" as synonyms: "*the protection of computer systems from the theft of or damage to their hardware, software, or electronic data, as well as from the disruption or misdirection of the services they provide*".[14] Consequently, in this case definitions for cybersecurity move decidedly from "*things that are done to protect*" or "*a state of being protected*" to "*protection of computer systems*", therefore to the aims of cybersecurity.

Indeed, describing its aims seems the preferred way to define cybersecurity today. In the words of Singer and Friedman, "*the canonical goals of security in an information environment result from this notion of a [cyber]threat. Traditionally, there are three goals: Confidentiality, Integrity, Availability, sometimes called the "CIA triad"*".[15] The CIA triad denotes any and all actions that are aimed at creating and preserving the confidentiality, integrity and availability of the underlying information technology asset. The CIA triad, that originated from a combination of academic papers and expert reports,[16] was widely adopted and finally found its way into EU law, that also added to the triad the concepts of resilience[17] and authenticity.[18]

The formal definition of cybersecurity, however, in EU law is found in the text of the EU Cybersecurity Act: "*cybersecurity means the activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats*" (Art. 2.1). Although the significance of this wording will be elaborated under subsection 2.1, here it is enough to be noted that EU law, while adopting the "*protection of network and information systems*" approach above and thus the CIA triad, also stresses that cybersecurity protects not only information systems, but also (and perhaps more importantly) persons, regardless whether users of such systems or third parties affected in any way by cyber threats.

A noteworthy definitional approach to cybersecurity comes from the CEN–CENELEC Focus Group on Cybersecurity (created by the European Standardization Organizations CEN, CENELEC and ETSI in 2011) that released a report in 2016[19] in response to EU's Cybersecurity Strategy. The report approached the term from a more technical than conceptual point of view,[20] focusing on cataloguing threats and risks. Its

[8] See, for example, Atle Refsdal A, Solhaug B, Stølen K, "Cybersecurity", in Cyber-Risk Management, SpringerBriefs in Computer Science. Springer, 2015; Schatz D, Bashroush R, Wall J, "Towards a More Representative Definition of Cyber Security", Journal of Digital Forensics, Security and Law: Vol. 12 : No. 2, 2017; Bay M, "What is cybersecurity – In search of an encompassing definition for the post-Snowden era", French Journal For Media Research, 6/2016; Kosseff J, "Defining Cybersecurity Law", 103 Iowa L. Rev. 985 (2017-2018); Maldonado R et al, "A simple definition of cybersecurity", Sociology Compass, 1(3), 2016; Kasper A, Antonov A, Towards Conceptualizing EU Cybersecurity Law, ZEI, 2019; Heim T N, Wessel R A, The Global Regulation of Cybersecurity: A Fragmentation of Actors, Definitions and Norms, in Lucía Millán Moro and Gloria Fernández Arribas (eds.), Ciberataques y Ciberseguridad en la Escena Internacional, 2020.

[9] Merriam-Webster Dictionary, accessed in Spring 2020 (https://www.merriam-webster.com/dictionary/cybersecurity).

[10] Cambridge Dictionary, accessed in Spring 2020 (https://dictionary.cambridge.org/dictionary/english/cybersecurity)

[11] Dictionary.com and Oxford University Press, accessed in Spring 2020 (https://www.dictionary.com/browse/cybersecurity?s=t).

[12] See US National Institute of Standards and Technology and US Committee on National Security Systems (information from CEN/CENELEC CSCG, footnote nr. 19).

[13] Encyclopaedia Britannica, accessed in Spring 2020 (https://www.britannica.com/search?query=cybersecurity).

[14] Wikipedia, accessed in Spring 2020 (https://en.wikipedia.org/wiki/Computer_security) .

[15] Singer P W, Friedman A, Cybersecurity & Cyberwar, Oxford University Press, 2014, p.35.

[16] See, for example, Fruhlinger J, "The CIA triad: Definition, components and examples", CSO, 10 February 2020 (https://www.csoonline.com/article/3519908/the-cia-triad-definition-components-and-examples.html).

[17] See footnote nr. 30 on the subject-matter and scope of the NIS Directive, and also Singer/Friedman, supra.

[18] See Michels J, Walden I, Beyond "Complacency and Panic": Will the NIS Directive Improve the Cybersecurity of Critical National Infrastructure? European Law Review, 2020, p.28.

[19] CEN/CENELEC CSCG, "Recommendation #2: Definition of cybersecurity", v01.08.

[20] See, for example, ibid, p.12.

recommendation is that there is no need for a definition of cybersecurity, at least "*not in the conventional sense that we tend to apply to definitions for simple things like authentication of an identity. The problem is that cybersecurity is an enveloping term and it is not possible to make a definition to cover the extent of cybersecurity coverage*".[21] Instead, "*a contextual definition is relevant, fits and is already in use*".[22] This approach, under the exact same wording, had been earlier also suggested by ENISA,[23] which had anyway taken active part in the above standardisation work.

In legal theory, Schatz, Bashroush and Wall have applied a computational approach to define cybersecurity as "*the approach and actions associated with security risk management processes followed by organizations and states to protect confidentiality, integrity and availability of data and assets used in cyber space. The concept includes guidelines, policies and collections of safeguards, technologies, tools and training to provide the best protection for the state of the cyber environment and its users.*"[24] Their result, while successful in identifying the common denominator, has provided, however, a text akin more to a concept[25] than a definition.[26] Similarly, Fuster and Jasmontaite found that "*the term 'cybersecurity', from an EU perspective, entails a combination of cyber resilience, cybercrime, cyber defence, (strictly) cybersecurity and global cyberspace issues*".[27] In addition to the above, many authors consider controlling user actions (through training or security control) as a core element of cybersecurity.[28] These attempts in essence illustrate the definitional impasse and perhaps justify the ENISA and CENELEC view that a definition for cybersecurity, it being an "*enveloping term*", may not be necessary because it is impossible.

Is a definition for cybersecurity necessary? Or, the fact that it is impossible to achieve makes this task obsolete? A first reply comes from EU law itself: the fact that a definition is included in the EU Cybersecurity Act demonstrates that EU legislators do not think this task is unattainable. However, there is also a functional reason justifying all attempts to define cybersecurity: the need to understand the term better. In Odermatt's words, "*without a clear definition of cybersecurity and its key terms, it is difficult for the EU to establish a comprehensive vision*".[29] A definition does not only warrant a standard way of reference but also helps to shed light onto the defined term. The list of definitions above already demonstrates basic differences in perspective: to some cybersecurity denotes measures and actions, to others a *state* of being protected, to others an ability to resist, and, to those adhering to the CIA triad, a set of aims and purposes. These are fundamentally different approaches. Notwithstanding the fact that professionals and theorists (information technology specialists, lawyers, social scientists, philosophers) may attach their own specific content onto cybersecurity, it is of fundamental importance to be clear on such basic distinctions as to whether cybersecurity is a set of actions, a *state* or both. This distinction will be elaborated in detail in the subsections that immediately follow.

2.2. *Cybersecurity as* praxis: *who are the cybersecurity addressees and recipients? What is its subject-matter and protective scope?*

Cybersecurity as *praxis* includes all actions and measures undertaken by the cybersecurity addressees in order to achieve the cybersecurity aims. *Praxis* therefore includes actionable items: originating from that set of cybersecurity definitions examined above that are based on "*measures taken to protect*" or "*things that are done*", cybersecurity as *praxis* denotes acts to serve a purpose. These acts are carried out by the cybersecurity addressees, the designated actors in cybersecurity rules and regulations. The aims of cybersecurity are set each time in the respective regulatory documents and may differ amongst them including anything from the confidentiality, integrity and availability of data and services[30] to a more general approach such as the one adopted in the EU Cybersecurity Act against "*cyber threats*". The measures and actions to achieve them may include processes, organisational measures taken in the natural or the digital world, the implementation of security software systems etc.

Because cybersecurity as *praxis* is very much dependant on an underlying information technology asset, which at times may constitute the main consideration for those involved in providing it, it is considered important to clarify cybersecurity's theoretical basis and components. The topic as practiced today being highly specialist and technical, and given also the above definitional divergences, an analysis of its theoretical constituting parts is believed to benefit all stakeholders. Closer examination of the cybersecurity addressees and recipients as well as of its subject-matter and scope is believed to be critical not only in creating better understanding on the exact content of cybersecurity but also in providing sound theoretical groundwork to those involved in providing it.

[21] Ibid, p.38.
[22] Ibid.
[23] See ENISA, "Definition of Cybersecurity", v1.0, December 2015, p.26.
[24] Schatz D, Bashroush R, Wall J, supra, p.66.
[25] Something that the authors themselves identify in their article, ibid.
[26] See also the definition of cybersecurity by Craigen D, Diakun-Thibault N, Purse R as "*the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights*" ("Defining Cybersecurity", Technology Innovation Management Review, October 2014, p.17).
[27] Fuster G G, Jasmontaite L, "Cybersecurity Regulation in the European Union: The Digital, the Critical and Fundamental Rights", in Christen M et al. (eds.), The Ethics of Cybersecurity, The International Library of Ethics, Law and Technology, Springer, 2020.
[28] See Breitinger F, Tully-Doyle R, Hassenfeldt C, "A Survey on Smartphone User's Security Choices, Awareness and Education", Computers & Security, (88)2020; Eichelberg M, Kleber K, Kämmerer M, "Cybersecurity Challenges for PACS and Medical Imaging", Academic Radiology, 27(8), 2020; Schnier B, Click Here to Kill Everybody, W.W. Norton & Company, 2018, p.45.
[29] Odermatt J, "The European Union as a Cybersecurity Actor", in Blockmans S, Koutrakos P (eds.), Research Handbook on EU Common Foreign and Security Policy, Edward Elgar Publishing, 2018.
[30] The "subject-matter and scope" of the NIS Directive is "achieving a high common level of security of network and information systems", whereby "'security of network and information systems' means 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 data" (Art.4.2).

In this context, cybersecurity as *praxis* needs to answer three critical questions for its content to be better understood: first, who are the cybersecurity addressees? Second, who are the cybersecurity recipients? Third, what is cybersecurity's subject-matter and protective scope?

As regards its addressees, cybersecurity as *praxis* could conceptually either include everybody or pertain only to a few. Under a participatory approach everybody would somehow need to act or carry out measures: individuals and legal persons would have to take action, as prescribed by law or other regulations, in order for each to contribute proportionately to achieving the cybersecurity aims. For example, organisations would need to implement technical and organisational measures and individuals would have to apply so-called "cyber hygiene" practices. Altogether, these collective measures would be aimed to serve the cybersecurity aims. Such an all-encompassing model would in effect resemble real-world security practice, whereby every organisation needs to take security-related measures and individuals need to lock their doors.

Conversely, under a restrictive approach only a few designated actors would be the cybersecurity addressees. Under this approach cybersecurity as *praxis* would not be addressed to everyone but would rather be a closed matter. Concrete actions would need to be taken by the designated few, who for some reason have been singled out and for whom a policy decision has been made that they are the only ones that need to act. For example, cybersecurity as *praxis* could be addressed only to a few organisations (critical infrastructures or other), that would need to apply technical and organisational measures.

As regards the cybersecurity recipients (natural and legal persons to the benefit of which cybersecurity addressees are called to act) here again an all-encompassing policy option would mean that everybody has an expectation to cybersecurity while a restrictive policy would limit the cybersecurity recipients to only a few. The exact content of such an expectation to cybersecurity will be elaborated in the subsection that immediately follows, where cybersecurity as a *state* will be discussed. Here it is enough to be noted that, while legislators and policymakers are of course free to decide, the nature of cybersecurity as a *state* and its broad connection to security most likely prejudice its circle of recipients. In other words, everybody who is active digitally, natural and legal persons alike, should be considered a cybersecurity recipient. The expectation to a *state* of cybersecurity cannot justifiably be confined to a closed set of natural or legal persons.

Finally, as regards its subject-matter and protective scope, the question here is what cybersecurity as *praxis* actually protects. In other words, if its aims are taken for granted, why have they come to be? Why do legislators, policymakers and information technology professionals go at such great lengths to protect the confidentiality, integrity and availability of data and services? For the sake of data and services themselves? Or, for the sake of network and information systems? Or, perhaps, for the sake of natural and legal persons?

"*Network and information systems*"[31] cannot be the subject-matter of cybersecurity. The protection of a computer system cannot be an end in itself. A "*network and information system*" is essentially hardware, a tangible system composed of microchips, hard drives, cables, etc. As such it is similar to an equally complex tangible system such as a car, a plane or (if we are to remain within a security context) a bank safe. Although a multitude of laws and regulations are in place prescribing how to manufacture a car or a plane or a bank money safe, neither the car, nor the plane or the money safe are the ultimate objects of protection of these laws: It is passengers (people) or money (property). In other words, the hardware is the means through which to access the data, not an end in itself.

Could then data be the subject-matter of cybersecurity? Data,[32] being the tangible target of cyber threats, easily pass the threshold of hardware as a means to a purpose discussed above. However, legal systems do not protect property as an end in itself: property is invariably protected in relation to its owner. In the above example of the bank money safe the equivalent would be that money is the recipient of all rules and regulations of bank law. This, of course, is not the case. In fact, it is the protection of the economy, as a basic societal component, that is the actual subject-matter of the relevant laws. Similarly, in the case of data, although they are protected within a cybersecurity context, it is persons having a right or a connection with them that are ultimately protected.

Natural and legal persons are therefore the subject-matter of cybersecurity as *praxis*. They occupy its protective scope.[33] It is to their benefit that cybersecurity addressees are called to act.[34] If cybersecurity as *praxis* achieves its aims, it will be natural and legal persons that will be in the position to feel this security, to confirm that cybersecurity as *praxis* has succeeded. Persons are the recipients of cybersecurity as *praxis*, they are

[31] It is understood that under Art 4.1 of the NIS Directive "network and information systems" also include "data"; However, only for the purposes of this analysis such "data" are not taken into consideration.

[32] At this point an important distinction needs to be made between data and information. In Floridi's words, as regards a General Definition of Information "*over the last three decades, several analyses in information science, in information systems theory, methodology, analysis and design, in information (systems) management, in database design, and in decision theory have adopted a General Definition of Information (GDI) in terms of data + meaning*"; similarly, "*it is common to think of information as consisting of data*" (The Philosophy of Information, Oxford University Press, 2011, pp.83ff.). While the philosophical extensions of this distinction exceed the purposes of this analysis, here it is enough to be noted that the cybersecurity objectives most likely refer to data rather than information in the above meaning.

[33] Accordingly, Kulezsa suggests a definition for cybersecurity ("*all measures aimed at protecting computer networks and digitized data from cyberthreats, including cybercrimes and other harmful activities*"), adding however that in order for "*the definition of cybersecurity to be useful it ought to cover only those threats that potentially bring harm to more than one individual – preferably a large number of people – or hold the potential to inflict significant material damage*" (Kulesza J, "Defining Cybersecurity", in Kulesza J, Balleste R (eds.), "Cybersecurity and Human Rights in the Age of Cyberveillance", Rowman & Littlefield, 2016, p.31).

[34] See also Kasper A, Antonov A, supra.

the ones to the benefit of which others (or even themselves) have to act.

Having established the theoretical groundwork for cybersecurity as *praxis*, a clear distinction needs to be made with actual cybersecurity practice today. As it will be later demonstrated (in subsection 2.1), the topic has developed, both from a technical and a legal perspective, into a highly technical one focused on IT assets and (critical) infrastructures. This is a development that is most likely consistent with the early stages of cyberattacks and cybercrime, when cybersecurity threats and attacks were expectedly placed on expensive or important targets that promised maximum return. Therefore, from this point of view actual practice has perhaps blurred the greater cybersecurity picture, drawing attention away from its actual subject-matter and protective scope. Nevertheless, once cyberattacks have entered the mainstream, as is perhaps gradually becoming the case today,[35] then cybersecurity will need to become universally applicable to all people and all systems in the same manner as a general right to security forms today an integral part of their everyday lives.

2.3. *Cybersecurity as a* state *to be protected by a right; would the general right to security suffice?*

Cybersecurity as a *state* is met when cybersecurity as *praxis* has achieved its purposes. In other words, if cybersecurity as *praxis* has achieved its protective scope (the actions and measures undertaken by the cybersecurity addressees in order to achieve the aims of cybersecurity have been successfully implemented and remain unchallenged), a *state* of cybersecurity ensues for the cybersecurity recipients. Once within this protective sphere of cybersecurity, natural and legal persons may enjoy a *state* of cybersecurity, having the expectation that they are, and remain, (cyber)secure. Or, it is a sphere within which protection is afforded to natural and legal persons from cyber threats, either present or potential.

The *state* of cybersecurity is of course a theoretical construct. It can be imagined as a sphere of protection within which the recipients of cybersecurity are allowed to enjoy unhindered a *condition* of cybersecurity.[36] Within it, their data and themselves are protected against any cyber threats. Each recipient of cybersecurity (individuals or organisations) has full control over its own respective sphere: it can, or should, take measures to protect it.[37] Third parties need to respect and comply with its will. However, being a theoretical construct, a *state* of cybersecurity does not necessarily include a successful attainment of its aims and purposes. In other words, a state of cybersecurity denotes only a claim to a sphere of protection; whether its recipients have achieved it not, whether they "have" cybersecurity or not, depends entirely on their actions – and the legal means provided to them to achieve it, as it will be later explained, under section 2.

It is at this point where the "*ability to protect or defend*", as identified in US cybersecurity standards (see above under 1.1), proves useful. An "*ability to protect or defend*" assumes a protective sphere, something to actually protect or defend. This protective sphere needs to have boundaries that are distinguishable to its recipient and to third parties. In addition, an "*ability to protect or defend*" includes both a will and the means to do so. If the will is taken for granted within a *state* of cybersecurity, the means through which to accomplish this need to be better approached. Means afforded to the cybersecurity recipients in order to defend their cybersecurity *state* may be legal and/or organisational/technical. Legal means would unavoidably involve a right to enjoy a *state* of cybersecurity (a right to cybersecurity) and an obligation of third parties to respect it. Organisational/technical means involve protective techniques and procedures. However, these measures are different than the ones implemented at the stage of cybersecurity as *praxis*. During the *praxis* stage the cybersecurity addressees needed to act in order to create a protective sphere. Once cybersecurity as a *state* has been created, the same or additional addressees (or even the cybersecurity recipients themselves) need to take the same or a different set of actions in order to preserve it.

Acknowledgement of a *state* of cybersecurity unavoidably affects both the cybersecurity addressees and the cybersecurity recipients. Although a *state* of cybersecurity could well be the result of actions of a few (e.g. critical infrastructures' organisations) while everybody else merely keeps an expectation for them to act, once cybersecurity as a *state* has been achieved its preservation may no longer burden only the few that helped create it. In other words, policy choices during the *praxis* stage do not need to prejudice policy choices once cybersecurity as a *state* has been created.

Far more important, however, is the fact that acknowledgement of a *state* of cybersecurity is critical in the formulation of a right to cybersecurity. Rights are "*entitlements (not) to perform certain actions, or (not) to be in certain states; or entitlements that others (not) perform certain actions or (not) be in certain states*".[38] Similarly, the Oxford English Dictionary provides the definition of a right (also as) "*the state of being entitled to a privilege or immunity or authority to act*". While a number of distinctions and categorisations has been suggested by rights' philosophers and legal theorists, common amongst most is a protected sphere placed at the control of the right's recipient: an "*immunity*" under the Hohfeldian system,[39] or a "*passive right*" under the active and passive rights distinction,[40] or a "*negative right*" under the positive and negative rights cat-

[35] See, for example, How Cyber-Attack Automation Turned SMEs into Sitting Ducks: And How to Change This, Liron Barak, InfoSecurity Magazine, 23 April 2021.

[36] On the "objective enjoyment" of a right being preferably the norm in society, see Donnelly J, Universal Human Rights in Theory and Practice, Cornell University Press, 2013, p.9.

[37] From this point of view cybersecurity as a *state* is different to the concept of cyber vigilantism, that is defined by K. K. e Silva as "*a social movement composed by individuals or collective groups who respond via technical means to a perceived and repercussive criminal act against the security of the Internet and information systems*" ("Vigilantism and cooperative criminal justice: is there a place for cybersecurity vigilantes in cybercrime fighting?", International Review of Law, Computers & Technology, Vol. 32 No. 1., 2018).

[38] See the Stanford Encyclopedia of Philosophy, "Rights", https://plato.stanford.edu/entries/rights/.

[39] See Hohfeld W N, Fundamental Legal Conceptions Applied to Judicial Reasoning, Yale University Press, 1919.

[40] See Lyons D, "The Correlativity of Rights and Duties", Noûs, 4: 45–57 (1970).

egorisation.[41] Common to all the above is acknowledgement of a *state*, a normative situation that cannot be affected or altered in any way without the consent of the rightholder. For the purposes of this analysis, a right to cybersecurity would effectively mean the rightholders' claim that their *state* of cybersecurity, as created by cybersecurity as *praxis*, remains intact by infringements and cyber threats.

Nevertheless, the question now is, what is the relationship between cybersecurity and security? Would general protection of the security of natural and legal persons be enough to also cover for cybersecurity? Or is introduction of a separate right, especially for cybersecurity, needed?

If one simply removes the "cyber" prefix from the definition given to cybersecurity in the EU Cybersecurity Act the result would read: "*security means the activities necessary to protect assets, their users and other persons by threats*".[42] This forms a good definitional approach to security: the Cambridge Dictionary defines "security" as "*protection of a person, building, organization, or country against threats such as crime or attacks by foreign countries*".[43] Consequently, a reasonable assumption would be that cybersecurity is nothing different than real-life security projected onto the digital realm. Or, in other words, that cybersecurity is a subset of security, promising individuals that they will be as secure in the digital world as they are in the real world. Hence, under the same assumption, there would be no need for a new right to cybersecurity because the general right to security is enough.

In the real world the individual right to security is a fundamental human right.[44] Human rights' theory[45] suggests that the right to security constitutes a "*basic*" human right, because it is necessary for other fundamental human rights to be meaningful and even possible. It is therefore claimed to take precedence over other human rights, because its "*enjoyment is essential to the enjoyment of all other rights*"[46] or "*no-one can fully enjoy any right that is supposedly protected by society if someone can credibly threaten him or her with murder, rape, beating, etc., when he or she tries to enjoy the alleged right*".[47]

However, interpretational difficulties quickly become noticeable: security can be threatened and destroyed by other than human agents, for example natural disasters, foreign states etc. In addition, the right to security can become difficult to clearly distinguish from the equally basic rights to life, liberty and even property. Each one of them may be interpreted not only as a right to be protected but also as a request to be provided with protection.[48] In the words of Lazarus, "*for the purposes of clarity, therefore, it makes sense to distinguish at the outset between a justiciable right to security; a non-justiciable right to security that is supported by non-judicial compliance mechanisms; the expression of a human rights standard or aspiration within an institutional context; and the expression of a human rights aspiration within political rhetoric or philosophical discourse. The 'right to security' is expressed in all of these contexts*".[49] All these considerations have led in the culmination of a new academic field, namely security studies ;[50] security studies approach security as a concept, and not as a fundamental human right alone.[51]

This approach echoes ENISA's definitional approach to cybersecurity, as seen above under 1.1, that, it being an "*enveloping concept*", it is impossible to define exactly.[52] Cybersecurity and security would then seem to share the same definitional and contextual difficulties. This finding, however, delineates the relationship between the two: security is not a parent concept to cybersecurity.[53] Instead, the two concepts are independent from each other.[54] Security is a fundamental human right and a concept that finds meaning based on the different contexts it is met. Cybersecurity may lack today the status of a human right, but it too finds meaning depending on the different contexts it is met. The two concepts differ, because security includes real-world circumstances, protecting against real-world threats, while cybersecurity refers to the digital realm, protecting from cyber threats.[55] The two sets of threats do not necessarily coincide. While a time may

[41] See Berlin I, Two Concepts of Liberty in Four Essays on Liberty, Oxford University Press 1969, p.118.

[42] See Article 2.1 of the EU Cybersecurity Act, admittedly having replaced the "*network and information systems*" with "*assets*", as transposed from the digital realm to the real world.

[43] Cambridge Dictionary, accessed in Spring 2020 (https://dictionary.cambridge.org/dictionary/english/security).

[44] See Article 3 of the Universal Declaration of Human Rights. In Europe, see Article 5 of the ECHR and Article 6 of the EU Charter of Fundamental Rights.

[45] Within the context of distinguishing between positive and negative human rights; On security see in particular Fredman S, "The Positive Right to Security", in Goold B J, Lazarus L (eds.), Security and Human Rights, Hart publishing, 2007 pp.307ff.

[46] Shue H, Basic Rights: Subsistence, Affluence, and U.S. Foreign Policy, Princeton University Press, 1980, p.20

[47] Ibid, p.21.

[48] All of the above arguments in Boersma David, Philosophy of Human Rights, Westview Press, 2011, p.83.

[49] Lazarus L, "Mapping the Right to Security", in Goold B J/Lazarus L (eds.), supra, p.330.

[50] "*Security studies exists as a subfield of international relations within political science, and in recent decades, the field has been expanded with theories of a more critically theoretical nature, linking it to more traditional areas of critical studies*", Bay M, supra, pp.9ff., with further references.

[51] See also Wessel R A, who suggests that cybersecurity triggers a new field of research in European law and policy, and even European Studies (Wessel R A, "Cybersecurity in the European Union: Resilience through Regulation?" in Conde E, Yaneva Z, Scopelliti M (eds), Routledge Handbook of EU Security Law and Policy, Routledge, 2019, pp. 283-300).

[52] As noted by ENISA "*A plea was made to stop the use of cyber as a general-purpose prefix but that appears to have fallen on deaf ears. The end-result is that removing the prefix and accepting that today the internet and electronic communication and control are endemic really means that cyber-security has the same difficulty in finding a simple definition as security*" (ENISA, supra, p.10).

[53] However, see also van de Poel I, "Core Values and Value Conflicts", in Christen M et al. (eds.), The Ethics of Cybersecurity, The International Library of Ethics, Law and Technology, Springer, 2020.

[54] See also the European Commission's distinction between "physical security" and "cybersecurity" in the Explanatory Memorandum of its its NIS 2 draft (Proposal for a 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, COM/2020/823 final, "the NIS 2 draft Proposal").

[55] See also Wessel R A who finds that "*part of the [European Commission's] Cybersecurity Strategy is related to linking core EU values that exist in the 'physical world' to the 'digital world'*" (Wessel R A, "European Law and Cyberspace", in Tsagourias N and Buchan R (eds.), International Law and Cyberspace, Edward Elgar Publishing, 2021.

well be imagined that the real and the digital converge, until such time cybersecurity and security, although sharing the same linguistic root and interpretational difficulties, should be treated as two different concepts and rights, each to be assessed by its own merit.

3. Putting theory to work: the need to introduce a new right to cybersecurity in eu law

Having established the two facets of cybersecurity, as *praxis* and as a *state*, the next step is to apply this distinction to the relevant regulatory approach applied so far in the EU. The aim is to identify the current state of play and to examine how the legislative provisions in effect today justify, or not, a claim for introduction of a new right to cybersecurity in EU law. Recourse, in the sense of a neighbouring *model par excellence*, will be sought in the field of EU personal data protection law.

To-date the EU has enacted two horizontal cybersecurity regulatory instruments, the NIS Directive (that is in the process of being amended through the, sequentially named, NIS 2 Directive) and the EU Cybersecurity Act, and has also established an EU Cybersecurity Agency (ENISA). These basic texts of reference are complemented with numerous case-specific regulations,[56] as well as, a number of cybersecurity provisions to be found in legislative texts of different subject-matter.[57] Non-regulatory instruments adding clarity and case-specific guidance to the field include the work by ENISA and various standards organisations and stakeholders.

For the purposes of this analysis, however, attention will be given only to the basic EU law texts on cybersecurity, namely the NIS Directive and the EU Cybersecurity Act. This will be done because these are the only EU regulatory texts of horizontal effect in force today. These two instruments are also interconnected, in the sense that the Cybersecurity Act refers to the NIS Directive as the "*Union's first legal act in the field of cybersecurity*".[58] An equally pragmatic reason refers to the fact that the European Commission itself identifies them as its basic cybersecurity legal tools in its relevant webpages.[59]

3.1. *The development of the eu regulatory framework on cybersecurity*

Under the distinction introduced in Section 1 cybersecurity may be understood as cybersecurity as *praxis* and cybersecurity as a *state*. This distinction was considered necessary, first, in order to better approach a multi-faceted term whose many contexts has created lack of clarity and, second, in order to highlight the necessary components of a new right to cybersecurity. Attention to its particulars (the cybersecurity addressees and recipients, its subject-matter and objectives) also provides a new perspective while examining the performance and interplay between the EU cybersecurity regulatory instruments currently in effect. As it will be demonstrated, EU cybersecurity law is (perhaps inconspicuously) steadily developing from standalone technical and organisational laws into a comprehensive regulatory approach.

The NIS Directive lays down obligations for all Member States to adopt a national strategy on the security of network and information systems, creates new organisations to develop trust and confidence (the NIS Cooperation Group and the CSIRTs network), introduces obligations for Operators of Essential Services and for Digital Service Providers, as well as, lays down obligations for Member States to designate national competent authorities, single points of contact and CSIRTs.[60] The NIS Directive builds on the Cybersecurity Strategy of the European Union issued in 2013 and also, although not directly related to it, on an older Directive on critical infrastructures,[61] that still remains in effect until today.

If put under the cybersecurity as *praxis* and as a *state* lens, a number of issues could be identified with regard to the NIS Directive's approach: First, as regards the cybersecurity addressees, the NIS Directive adopts a limited-circle policy approach. It is addressed only to a closed number of actors, essentially Digital Service Providers and Operators of Essential Services, as well as, to Member States and the EU itself. These are expected to take specific actions at the cybersecurity as *praxis* stage, leaving all other stakeholders unaffected. In essence, only a handful of organisations are expected to take any cybersecurity action under the NIS Directive. Its policy option is not to impose a horizontal approach onto EU societies, whereby everybody would have to act in one way or another, but instead to focus on a very limited circle of cybersecurity addressees.

Similarly, the NIS Directive makes no reference to any cybersecurity recipients. Its provisions are open-ended, in the sense that they do not, explicitly at least, name any recipients; legal obligations placed upon its addressees are not introduced to the benefit of any specifically-named natural or legal person. They do not create any rights to any third parties. Accordingly, the NIS Directive does not confer any rights or other means of protection to the persons (legal or natural) whose rights will be infringed if its addressees do not perform their legal duties. If cybersecurity as *praxis* fails because the NIS Directive addressees infringe its provisions, those affected by this infringement are not enabled to act in any manner. Ar-

[56] An indicative list would include Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (OJ L 345, 23.12.2008, p. 75–82), or Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA (OJ L 218, 14.8.2013, p. 8–14),

[57] See, for example, Annex I of the EU Regulations on medical devices 745/2017 (MDR) and 746/2017(IVDR).

[58] Recital 15 of the EU Cybersecurity Act.

[59] See, for example, https://ec.europa.eu/digital-single-market/en/policies/cybersecurity

[60] Art. 1.2 of the NIS Directive; See also Markopoulou D, Papakonstantinou V, De Hert P, "The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation", Computer Law and Security Review, Vol. 35 Issue 6, November 2019.

[61] Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.

ticles 15 and 17 of the NIS Directive[62] merely grant national supervisory authorities with the power to "issue binding instructions" or ask to "remedy failures".

As regards the NIS Directive's subject matter and scope, in its own wording "*this Directive lays down measures with a view to achieving a high common level of security of network and information systems within the Union so as to improve the functioning of the internal market*" (Art. 1.1).[63] Therefore, it is the "functioning of the internal market" upon which the release of the NIS Directive is based and not the protection of natural and legal persons *per se*. A "*high common level of security*" is to be achieved but this is not aimed at the benefit of any cybersecurity recipient but in order to "*improve the functioning of the internal market*".

Admitting that it exists for market purposes only, it is doubtful whether the NIS Directive contributes at all to the creation of a cybersecurity *state*. The fact that the NIS Directive carries no recipients and identifies only the "*functioning of the internal market*" as its *raison d'être* may be understood to mean that its aim is not to serve natural and legal persons' rights and interests in any way. Consequently, it would be only through an interpretational attempt that any protective scope other than for financial interests could be derived out of the NIS Directive: security of network and information systems[64] needs to be reached in order to "*improve the functioning of the internal market*"; public trust (as also identified in the EU Cybersecurity Act) is an integral component to achieving such "*improvement*" of the internal market, and, in turn, creation of a protective sphere and the establishment of cybersecurity as a *state* for natural and legal persons helps create such public trust.

However, this is the result of an interpretation. Based strictly on its wording, the NIS Directive constitutes a limited-scope legal tool, addressed only to a few actors, making no reference to any recipients and conferring no rights or creating no protection to anybody in the EU. The NIS Directive may be perceived as a technical, open-ended regulatory instrument aimed merely at improving network and information systems' operation so as to improve the market conditions within Europe. Nevertheless, this characterisation would largely defeat its perception in the EU: In the Commission's own words, admittedly retrospectively, "*in an effort to better protect citizens online, the Union's first legal act in the field of cybersecurity was adopted in 2016 in the form of Directive (EU) 2016/1148*".[65]

If that is actually the mindset behind its release and its public perception, then the NIS Directive needs to be applied under a much broader lens in order to support both cybersecurity as *praxis* and cybersecurity as a *state* considerations. Such an interpretation could be supported by the EU's approach on the cybersecurity instrument that followed the NIS Directive's release three years later, the EU Cybersecurity Act.

The EU Cybersecurity Act seems to amend the NIS Directive's shortcomings identified above and makes important contributions to cybersecurity in Europe, but does so in an unassuming manner. If assessed under word-count metrics, the EU Cybersecurity Act's provisions carry little justification to their title: rather than a list of rights and obligations, as would perhaps be the expected content in any legal "*act*", they constitute instead, first, the constitutional document of EU's Agency for Cybersecurity (ENISA), and, second, the incorporation framework for a European cybersecurity certification scheme. As regards ENISA, the EU Cybersecurity Act is simply the latest addition to its predecessors of 2004 and 2013,[66] that nevertheless did not carry such an attractive title; in fact, the word "*cybersecurity*" itself was not to be found at all in their text, despite of the fact that it was well-known and used at the time of their respective release. As regards the European cybersecurity certification scheme, the relevant provisions are only aimed at exactly that, the organisation, setup and operation of a new certification scheme in Europe.[67]

From this point of view the most pertinent provisions to the broader cybersecurity purposes in the EU Cybersecurity Act are to be found in its Articles 1 and 2, where its subject matter, scope and definitions are provided respectively. Although quite limited in length, the contribution of these few provisions is disproportionately important. As regards its subject matter and scope, the EU Cybersecurity Act is introduced "*with a view to ensuring the proper functioning of the internal market while aiming to achieve a high level of cybersecurity, cyber resilience and trust within the Union*" (Art. 1.1). Here too, as was the case in the NIS Directive, the EU's cybersecurity regulatory intervention is based on the "*proper functioning of the internal market*"; again, market considerations and not the protection of persons is the *raison d'être* of the EU Cybersecurity Act. Nevertheless, close comparison of Articles 1.1 of EU's two cybersecurity legal instruments demonstrates an important qualitative differentiation in the wording of the Cybersecurity Act: in its case the "*proper functioning of the internal market*" is to be achieved "*while*" aiming to achieve cybersecurity, cyber resilience and trust, placing therefore all four on the same level. On the contrary, in the NIS Directive security was to be achieved "*so as to improve*" the internal market, thus as merely a means to an end.

Similarly, the EU Cybersecurity Act provides a definition for cybersecurity in the EU. The boldness of this policy option ought not be overlooked: against formal recommendation by the very agency the Act creates as EU's Agency for Cybersecurity (see above under 1.1), and against all difficulties highlighted in dictionaries, academic papers and technical reports, the Act decidedly defines cybersecurity as "*the activities neces-*

[62] On "*implementation and enforcement*" for Operators of Essential Services and Digital Service Providers respectively.

[63] See also Fuster G G, Jasmontaite L, supra.

[64] In the sense of their "*ability […] to resist […] any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services […]*", Art. 4.2 of the NIS Directive.

[65] Recital 15 of the EU Cybersecurity Act (see also the Explanatory Memorandum of the NIS 2 draft Proposal) . However, even at the time of the Act's release the Commission thought that security of the digital environment "*can have a strong positive impact for the effective protection of fundamental rights, and specifically the right to the protection of personal data and privacy*" (reference in Jasmontaite L, Pavel Burloiu V, "Lithuania and Romania to Introduce Cybersecurity Laws", in Schünemann W J, Baumann M-O, Privacy, Data Protection and Cybersecurity in Europe, Springer, 2017, p.133, with further analysis of the NIS Directive provisions).

[66] Regulations 460/2004 and 526/2013 respectively, see also Recital 14 of the EU Cybersecurity Act.

[67] See Title III of the EU Cybersecurity Act.

sary to protect network and information systems, the users of such systems, and other persons affected by cyber threats" (Art. 2.1).[68] This definition, being included in EU's Cybersecurity Act, from now on constitutes the formal EU approach on this matter; all other texts and understanding in the EU ought to refer to it. Although the Act is not addressed at Member States, by way of indirect application (ENISA being EU's Agency for Cybersecurity and the certification scheme intended to run throughout Europe), it should be expected that they too will follow the Act's definitional approach.

Under the cybersecurity as *praxis* and as a *state* lens the Act at first sight appears to relate only to the former: cybersecurity is explicitly perceived as "activities". Action is anticipated *prima facie* when it comes to cybersecurity. A *state* of cybersecurity is not, expressly at least, acknowledged. However, an important component of the Act's definition is "*cyber threats*".[69] These are "*any potential circumstance, event or action that could damage, disrupt or otherwise adversely impact network and information systems, the users of such systems and other persons*" (Art. 2.8). What is of extreme importance for the purposes of this analysis is that "*persons*" are used in the Act both in the "*cybersecurity*" and in the "*cyber threat*" definitions :[70] persons are to be protected by cyber threats; and, cyber threats is anything that may disrupt or adversely impact a person. Combination of the two amounts to acknowledgement of cybersecurity as a *state*: a protective cybersecurity sphere created to the benefit of persons, within which they are protected, they cannot be "*damaged, disrupted or otherwise adversely impacted*". It should also be noted that these persons are not only the users of the relevant network and information systems but, explicitly, all persons indiscriminately – another indication of the EU Cybersecurity Act's intention to acknowledge cybersecurity as a *state*.

Having established that the EU Cybersecurity Act, although in a minimalistic way, has taken important steps towards understanding of cybersecurity in the EU both as *praxis* and as a *state*, it is much easier (but not less important) to divulge its contribution as regards cybersecurity's stakeholders. Here too important change is carried out in a subtle manner. As regards the cybersecurity's addressees, while specific reference is made to Operators of Essential Services and Digital Service Providers, as was the case in the NIS Directive, ENISA's mandate is much broader and is in no manner confined only to them.[71] ENISA has the mandate to assist or intervene, as appropriate each time, whenever a matter of cybersecurity arises in the EU, regardless of its origins. Nowhere in the EU Cybersecurity Act's text is it mentioned that only Operators of Essential Services and Digital Service Providers or even Member States or the EU are expected to act. Cybersecurity is treated instead as a global European concern: "*increased digitisation and connectivity increase cybersecurity risks, thus making society as a whole more vulnerable to cyber threats and exacerbating the dangers faced by individuals, including vulnerable persons such as children. In order to mitigate those risks, all necessary actions need to be taken to improve cybersecurity in the Union.*"[72]

An important further contribution of the EU Cybersecurity Act is that it moves decidedly away from the CIA paradigm. The cybersecurity aims in the EU are no longer the confidentiality, integrity, authenticity and availability of data and services as was the case under the NIS Directive. Instead, it is the protection of systems, users and persons by cyber threats. At a higher level, its aim is to "*achieve a high level of cybersecurity, cyber resilience and trust*". This is an important shift of perspective: the EU cybersecurity edifice moves from a technical objective-orientated system to a rights-based approach. The good standing of systems is set aside (or, more accurately, set as a technical, secondary objective within the EU certification scheme also introduced by the same Act), and the general cybersecurity approach is now rights-orientated. Data and services are no longer the EU cybersecurity aims but, instead, the creation of a protective sphere, whereby no "*circumstance, event or action*" could possibly "*damage, disrupt or otherwise adversely impact*" systems and, more importantly, persons. This is a further important step taken by the EU Cybersecurity Act towards acknowledgement of a right to cybersecurity in the EU.

In 2020 the Commission released its proposal for an amendment of the NIS Directive, to be sequentially named the NIS 2 Directive.[73] Although at the time of drafting this paper the NIS 2 Directive was still under the law-making process, it is already clear from the Commission's text that the NIS 2 aims to expand the NIS Directive and address its shortcomings,[74] taking however (what is most important for the purposes of this paper) the Cybersecurity Act's achievements for granted. Most notably, the NIS 2 draft Proposal employs the Act's definition of "cybersecurity" for its purposes.[75] Consequently, in spite of its technical character, the NIS 2 Directive, once it comes into effect, will also be aimed at protecting not only "*network and information systems*", but also "*the users of such systems, and other persons affected by cyber threats*". Similarly, while the NIS Directive's subject matter is to "*lay down measures with a view to achieving a high common level of security of network and information systems within the Union so as to improve the functioning of the internal market*", the NIS 2 Directive's scope, once it comes into effect, will be far more visionary: "*this Directive lays down measures with a view to ensuring a high common level of cybersecurity within the Union*", thus expanding its protective scope also to include individuals.

[68] See also Wessel R A, European Law and Cyberspace, supra.

[69] Moving cleverly in this manner away from the connection of cybersecurity exclusively with cybercrime (for this connection see, for example, European Commission, Eurobarometer 464a, supra); While all cybercrime are expected to infringe cybersecurity, not all cyberthreats are cybercrimes (see also Kulesza J, supra, p.30).

[70] A point also identified in Kasper A, Antonov A, supra.

[71] See, above all, the EU Cybersecurity Act's Art 3.1 on the ENISA mandate, where no mention is made to a closed set of addressees – in fact, quite the opposite is the case.

[72] Recital 3 of the EU Cybersecurity Act.

[73] The NIS 2 draft Proposal.

[74] See the Explanatory Memorandum of the NIS 2 draft Proposal (in particular, Chapter 1). Strangely, however, although the Commission admits that the NIS Directive was "the first piece of EU-wide legislation on cybersecurity" and the NIS 2 draft is intended to replace it, it is not classified as falling under the "area of cybersecurity" but instead under the "area of physical security" (see Chapter 1 of the Explanatory Memorandum, "Consistency with existing policy provisions in the policy area").

[75] See Art. 4.3 of the NIS 2 draft Proposal.

Other than the above changes, the Commission's draft proposal is aimed at addressing the identified[76] NIS Directive's shortcomings. In this context, while broadly following its structure, the NIS 2 Directive text is far more extensive than its predecessor, each one of its chapters being specifically aimed at resolving difficulties caused by the NIS Directive. Consequently, its Chapter I switches to "essential" and "important" entities as the NIS 2 Directive's recipients in order to deal with issues caused by its predecessor's categorisations. Chapter II details the requirements of Member States' national cybersecurity strategies, aiming at harmonisation and enhanced consistency, while at EU level improved cooperation and information exchange is intended to be achieved through Chapter III (and the introduction of yet another EU cooperation network).[77] The Cybersecurity risk management and reporting obligations are detailed under an, expansive, Chapter IV, which presumably needs to be read together with Chapter V on (extended) information sharing practices. Finally, Chapter VI focuses on supervision and enforcement – most notably, however, still staying short of awarding any remedies to individuals. At any event, regardless of its final formulation the fact remains that, as far as the purposes of this analysis are concerned, the NIS 2 draft Proposal builds on the EU Cybersecurity Act's *aquis*, and therefore creates an EU cybersecurity framework that, taking the cybersecurity definition into account, is ultimately aimed at protecting any *"person affected by cyber threats"*.

3.2. *Acknowledgement of a, new, right to cybersecurity in eu law*

As seen in the previous subsection, the EU Cybersecurity Act acknowledges and validates in a subtle manner cybersecurity both as *praxis* and as a *state* in the EU. Its definition of cybersecurity, applicable throughout the EU from now on, acknowledges both cybersecurity as *praxis*, in the sense that it includes all *"activities necessary to protect"* anybody (and anything) threatened by cyber threats, and cybersecurity as a *state*, in the sense that all *"persons"*, regardless whether systems' users or not, are entitled to protection from *"any potential circumstance, event or action"* that could *"adversely impact"* them in any way. This understanding of cybersecurity brought by the EU Cybersecurity Act constitutes an important step towards protecting the cybersecurity of all natural and legal persons in the EU through introduction of a new right to cybersecurity.

To the extent that this signals an intentional process by the EU legislator, as demonstrated by the evolution from the more technical NIS Directive to the aforementioned definition of cybersecurity in the EU Cybersecurity Act and the visionary aim-setting of the NIS 2 draft Proposal, it is important that law-making efforts continue at least in the same pace, if not escalate.[78] Shortcomings of the current EU regulatory framework on cybersecurity, particularly in terms of a patchwork, have been well-identified.[79] Despite repeated calls for a release of a comprehensive EU cybersecurity regulatory framework (in the form of an EU Cybersecurity Law) ,[80] this aim remains until today elusive: the EU Cybersecurity Act for the moment stays short of serving this purpose due to its predominantly functional character (being focused for most of its part on ENISA and the certification framework), while other cybersecurity-relevant legal provisions are found scattered in a multitude of legal documents of various legal statuses. Nevertheless, taking for granted the positive steps undertaken by the EU Cybersecurity Act already, the next conceivable stage for EU policy-making would be the formal acknowledgement of a right to cybersecurity. Such a right would be placed at the centre of the emerging EU Cybersecurity Law.

A number of reasons justifies the need for introduction of a, new, right to cybersecurity in EU law. First and foremost, despite of the fact that, as seen, cybersecurity as a *state* is acknowledged in the text of the EU Cybersecurity Act, individuals are not afforded with any legal means with which to protect it. The Act recognises a need to protect all *"persons"* against any *"event or action"* that could *"damage, disrupt or otherwise adversely impact"* them. In order to achieve this, all *"activities necessary"* need to be carried out, under a cybersecurity as *praxis* perspective. However, what happens if these activities either fail or are not undertaken at all?

Admittedly, if a cybersecurity threat is realised and, as a consequence, natural and legal persons are *"adversely impacted"*, it is most likely that other fields of law will apply to a lesser or greater extent, that afford protection to the persons concerned. If, for example, personal data are unlawfully accessed then the European Data Protection Regulation[81] will step in. If proprietary data are unlawfully used, then Intellectual Property Law (including the EU Database Directive)[82] may provide protection to the natural and legal persons concerned. Unfair competition, civil or even criminal law[83] could also, under certain conditions, step into the picture.

However, these legal safeguards are beyond the point of cybersecurity, both from the perspective of its addressees and from the viewpoint of its recipients. For cybersecurity addressees there is an issue of relevance: cybersecurity has been singled out as a separate and important policy field within the EU; a lot of resources and effort have been given into realis-

[76] Through *"evaluations and fitness checks"* run by the Commission and put forward in the NIS 2 draft proposal's Explanatory Memorandum.

[77] The cyber crises liaison organisation network (EU - CyCLONe), see Art. 14 of the NIS 2 draft Proposal.

[78] On the importance of the "normative role" of the state in cybersecurity see Cavelty M D, Egloff F J, "The Politics of Cybersecurity: Balancing Different Roles of the State", St Antony's International Review 15 no.1, 2019.

[79] See Porcedda M G, "Patching the patchwork: appraising the EU regulatory framework on cyber security breaches", Computer Law & Security Review, Vol. 34 Issue 5, 2018.

[80] See Kasper A, Antonov A, supra, Wessel R A, Cybersecurity in the European Union, supra, Fuster G G, Jasmontaite L, supra, Odermatt J, supra.

[81] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016on 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) (the "GDPR)".

[82] Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases.

[83] Again, under the clarification that not all cyber threats are cybercrimes.

ing a comprehensive policy; specialised administrative mechanisms have been installed both at EU and at Member State level: in the words of Wessel R A, "*cybersecurity forms an excellent example of an area in which the different policy fields of the Union need to be combined (a requirement for horizontal consistency), and where measures need to be taken at the level of both the EU and the Member States (calling for vertical consistency)*".[84] If no consequences are attached to default or negligence by its addressees, then a very concrete risk is raised that all these efforts do not develop their potential to the fullest extent possible.[85] Good regulation requires consequences to be attached to infringements of obligations. Otherwise, if addressees are not faced with concrete consequences, they may be tempted to be lax on their implementation of the EU cybersecurity requirements, in view of the costs and effort involved.[86]

From the cybersecurity recipients' perspective ("*users*" and "*persons*", in the wording of the EU Cybersecurity Act), whether other fields of law protect them anyway is irrelevant. A policy introduced to their benefit, specifically aimed at not damaging, disrupting or adversely impacting them in any way, cannot be applied without their awareness and in their absence. If left in its current wording, as set in the EU Cybersecurity Act, cybersecurity would be a remote concern to be exclusively handled within EU and Member State organisations, essentially a behind-closed-doors policy. Although important in its own merit, such a policy would fail to develop the impact aimed at individual level and would most likely fail to achieve "*trust within the Union*".

Consequently, a right to cybersecurity needs to be formally introduced in EU law as a means of empowering individuals in the digital realm. Individuals need to be able to protect themselves from digital (which is after all what the prefix "*cyber*" stands for) threats. Digital threats consistently occupy the highest places in the lists of concerns raised by individuals today.[87] They therefore need to be provided with the legal means to protect themselves by cyberthreats. This task should not be outsourced exclusively to their governments and the EU ;[88] each one needs to become aware of the threat and be afforded with the legal means to make sure that he or she is not "*damaged, disrupted or otherwise adversely impacted*" by it. A new right to cybersecurity would also induce so-called cyber-hygiene practices: in the same manner that individuals have learned to lock their doors and bicycles in real-life, participating thus in the creation of security for them, they also need to take measures to defend themselves in the digital realm, as assisted by the law.[89]

The law-making conditions to introduce a new right to cybersecurity in EU law are already available. As seen, the EU Cybersecurity Act has already paved the way. The basic components for introduction of a new right are already found in its provisions. Any new right would need to create obligations to an indefinite number of addressees and to protect an indefinite number of recipients. The EU Cybersecurity Act has accomplished exactly that: its definition of cybersecurity is open-ended, in the sense that it is neither addressed to a closed circle of actors nor is it restricted in its scope to a small circle of recipients. No longer are critical infrastructures, Operators of Essential Services or Digital Service Providers (or their replacements under the NIS 2 Directive) the only ones that need to act. Instead, anybody ought to undertake *"all activities necessary"* to protect from cyber threats. Similarly, everybody needs to be protected. The cybersecurity's definition in the Act applies to all persons, not simply the users of the systems under threat.

Accordingly, the EU Cybersecurity Act, by moving decidedly away from the CIA paradigm, has shifted towards a rights-based approach. No longer is EU cybersecurity aimed at the good standing of information technology systems, as was the case under the NIS Directive. Through the Act's provisions the aim of EU law is by now the creation of a protective sphene for any person, in which he or she cannot be adversely impacted in any way. In this manner again clear progress in the EU legislator\s mindset is viewable, from the technical premises of the NIS Directive to the ground-setting provisions of the Act, that are subsequently taken for granted by the NIS 2 draft Proposal.

Finally, the EU Cybersecurity Act placed on par the functioning of the internal market and the creation of trust in the Union. No longer are diverging cyber strategies by Member States that are distorting the internal market the only reason for release of cybersecurity legislation. Instead, the Act is also aimed to create trust to individuals across the EU. In this way it is not addressed only to organisations and governments but also to persons, who are the recipients of and need to feel such trust. In this manner, because the EU Cybersecurity Act has taken positive steps towards laying down the necessary theoretical groundwork, future introduction of a general right to cybersecurity in EU law has been made possible.

A new right to cybersecurity in the EU could, on the one hand, acknowledge an individual's right to defend itself against cyber threats and, on the other hand, place obligations to everyone else to respect it.[90] While the exact contents of such a new right are beyond the scope of this paper, here it is merely noted that such a right could be quite detailed or quite abstract and general. The former would mean that individuals would be afforded with specific rights, special to the cybersecurity conditions and threats, and that the cybersecurity addressees would have to demonstrate compliance by way of

[84] See Wessel R A, Cybersecurity in the European Union, supra.

[85] This problem has been identified in concrete with regard to the NIS Directive; the Explanatory Memorandum of the NIS 2 draft Proposal expressly states that "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. This can have negative consequences for the cyber resilience of individual entities".

[86] See also Fuster G G, Jasmontaite L, supra, on the "duty of care" principle, as well as, on the revision of the existing EU liability framework.

[87] See Recital 54 of the EU Cybersecurity Act.

[88] Without this precluding cyber-diligence measures from their part (see Bannelier K, Christakis T, Cyber-Attacks: Prevention-Reactions, The Role of States and Private Actors, Les Cahiers de la Revue Défense Nationale, Paris, 2017). Together with the "*duty of care*" on behalf of private enterprises and cyber-hygiene measures to be taken by individuals they could form the content of a new right to cybersecurity.

[89] See also Recital 8 of the EU Cybersecurity Act.

[90] On some, preliminary, thoughts see footnote nr. 90.

concrete actions and measures. The latter would simply acknowledge its existence, and leave it to individuals to remain vigilant and seek redress in front of courts in case of infringement.

Finally, the law-making means to introduce a new right to cybersecurity in EU law could, for example, include a relevant amendment of the EU Cybersecurity Act or the NIS (2) Directive in the sense that these are the two obvious candidate legal instruments currently in effect. Alternatively, a right to cybersecurity could be included as a special sub-category of the general right to security in the EU, perhaps by amending Article 6 of the EU Charter of Fundamental Rights. Nevertheless, in view of the difficulties in amending fundamental rights' texts and given also the ambitious naming of the EU Cybersecurity Act, it would perhaps be preferable if introduction of a new EU right to cybersecurity was performed through a future amendment of its provisions that could include a third part to cover this topic as well.

3.3. *The right to data protection as a* model par excellence *for cybersecurity in eu law, addressing the questions of legal basis and eu competence to act*

EU personal data protection presents stark similarities with cybersecurity. Because they both relate to the digital realm (admittedly, personal data protection exceeding it to include non-automated personal data processing under certain conditions)[91] they can be considered neighbouring fields.[92] Their shared origins has led to a shared cause: they both aim to protect individuals from risks caused by new technologies. In fact, the GDPR today could be claimed to be the standard EU regulatory mechanism to deal with anything from robots and artificial intelligence to biotechnology, big data or the internet of things.[93] Another common characteristic, perhaps stemming from their relationship with technology, is that they were both developed globally, in a cross-border manner :[94] Dealing essentially with international concerns at state and individual level, they have grown to the task of providing a global regulatory response. Finally, their mode of deployment is similar, in the sense that they both required a new administrative mechanism to be setup in order to serve their purposes.

Apart from similarities, cybersecurity and data protection differ most importantly in their scope: data protection has a much more limited scope, aimed only at the protection of personal data. Cybersecurity, on the other hand, is aimed at protecting "*persons*" against any cyber threat. In spite of personal data occupying a large portion of the digital realm (the EU having acquired its first non-personal data legislation as late as in 2018),[95] the fact remains that cybersecurity is all-inclusive while data protection is case-specific. The other significant difference refers to time precedence: data protection emerged as early as in the 1970s, while cybersecurity legislation is no older than the early 2000s, despite of the fact that the relevant risks were known at least since the 1980s. This has unavoidably affected the sophistication of each legal system: data protection in the EU is a complex legal system of more than twenty-five years of history and a second-generation text of law, while cybersecurity only got its first specifically-named legal text, the EU Cybersecurity Act, in 2019.

However, because of their significant similarities, it is possible that data protection in the EU could serve as a *model par excellence* for cybersecurity.[96] If this is the case then EU data protection could assist a (nascent) EU right to cybersecurity in two critical ways: the first refers to its legal basis and the second to EU law's competence to legislate in the cybersecurity field. In order to demonstrate how EU data protection law could assist in these matters attention shall be given to the 1995 EU Data Protection Directive.[97]

As far as identification of a suitable legal basis in EU law for development of a new right to cybersecurity is concerned, Article 114 TFEU could well suffice, if at least the EU personal data protection model can be used as evidence. The 1995 EU Data Protection Directive was released on the basis of Article 100a of the Treaty establishing the European Community, whose aim was the "*establishment and functioning of the internal market*", same as is the case today in the EU Cybersecurity Act.[98] As is known by now, the 1995 EU Data Protection Directive regulated personal data protection in Europe for several years, until the Treaty of Lisbon came in 2008 and explicitly introduced a new right to personal data protection. Consequently, the law-making process in EU law is not necessarily linear. In other words, it is not necessary first for a new right to be spelled out in the Treaties, in order for secondary legislation to further detail its particulars. As has personal data protection demonstrated, a Directive (or, a Regulation, for example the EU Cybersecurity Act) could well grant to Europeans rights and obligations akin to a right, before a right *per se* finds its way into the Treaties. Developments so far in EU law justify this approach. As seen, there is a clear development towards a more protective scope from the NIS Directive to the EU Cybersecurity Act. The latter, that shares the same legal basis as the 1995 EU Data Protection Directive (now, Article 114 TFEU),[99] could perhaps be amended in the future to include details of a new right to cybersecurity while still within its scope of pro-

[91] See Art. 2.1 of the GDPR, particularly with regard to "processing other than by automated means".

[92] See also Recital 15 of the EU Cybersecurity Act, where EU's data protection legal instruments are listed as also "*contributing to a high level of cybersecurity in the digital single market*", as well as, the Explanatory Memorandum of the NIS 2 draft Proposal.

[93] As demonstrable by simply consulting the exhaustive list of topics dealt with by the European Data Protection Board (that succeeded the Article 29 Data Protection Working Party), available at https://edpb.europa.eu

[94] See, indicatively, De Hert P, Papakonstantinou V, "Three Scenarios for International Governance of Data Privacy: Towards an International Data Privacy Organisation, Preferably a UN Agency?", I/S A Journal for law and Policy in the Information Society, Vol. 9 No. 13 (2013), pp.274ff.

[95] See Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union.

[96] A connection also identified in Fuster G G/Jasmontaite L, supra.

[97] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (the "1995 EU Data Protection Directive").

[98] The same legal basis has been employed by the Commission also for the NIS (and NIS 2 draft Proposal) Directives.

[99] See also Odermatt J, supra.

tection of the "*fundamental rights and freedoms*" of natural and legal persons.[100]

The second case where EU data protection law could substantially assist the birth of a new EU right to cybersecurity refers to addressing the basic question of EU law competence to legislate in the field.[101] The counter-argument in this case is that the EU is limited to introducing legislation to which it has either an exclusive or shared competence, and that cybersecurity falls outside the scope of EU law, being related to public and national security. In the, characteristic, words of Wessel R A, "*the fact that the European Union justified and clarified its legal activities in this area in a 110-points preamble to the EU Cybersecurity Act points to an awareness that this is not obvious area to deal with from a legal perspective*".[102]

Two points can be raised in this regard. First, that cybersecurity is such a broad concept that only parts of it fall outside EU law competence. Topics such as the harmonisation of the Internal Market or protection of the fundamental rights and freedoms of natural and legal persons do fall under EU law competence, and have actually already led to release of the NIS Directive and the EU Cybersecurity Act. While state security and criminal law may lie outside EU law competence, this does not preclude the EU legislator from introducing protective cybersecurity regulatory provisions, akin to a right, to the benefit of Europeans. As discussed above, EU personal data protection shows that the details of a new right may exist in EU law years before its formal acknowledgement in the Treaties.

The second point refers to the fact that, again taking EU personal data protection into consideration, fields within and fields outside EU law competence may co-exist under the same regulatory roof. Most notably, this is the case with EU personal data protection today. The 1995 EU Data Protection Directive expressly excluded itself from "*public security, defence, state security (including the economic well-being of the state when the processing operation relates to state security matters) and the activities of the state in areas of criminal law*".[103] A careful approach as regards state and national security was also maintained under the 2016 EU data protection reform package, despite of EU data protection's newly elevated status as a fundamental individual right :[104] both the GDPR and the LED ultimately excluded from their scope all fields not regulated by EU law. The above approach by EU personal data protection law demonstrates that co-existence under the same fundamental right of fields falling within and fields outside EU law competence is actually possible, under a careful balancing by the EU legislator to accommodate both. Similarly, EU competence to legislate in the cybersecurity field faces the same dilemma and follows the same methodology: Article 1.2 of the EU Cybersecurity Act sets that its provisions are "*without prejudice to the competences of the Member States regarding activities concerning public security, defence, national security and the activities of the State in areas of criminal law*" (Art. 1.2). The NIS Directive kept a cautious stance as well (see its Recital 8). Therefore, it could be claimed that EU cybersecurity is already following the path paved by EU personal data protection, towards eventual introduction of a new right that would at the same time respect EU competences to legislate.

4. Conclusion

Introduction of a new right into EU law is by no means an easy to accomplish task. However, a new right to cybersecurity does not build in void. In fact, its basic components are in place, EU law having already taken definite steps towards this direction: in spite of a global definitional impasse, it has boldly suggested a definition for cybersecurity in the most formal manner. Its definition is not only bold as an initiative but also forward-looking in its conception: rather than simply making use of well-known technical paradigms, it has adopted a rights-based approach. Similarly, cybersecurity as *praxis* is by now a well-known idea in EU law and practice, established in a multitude of legal texts and formal policies that are almost a decade old. Relatively recently, through a few but precious provisions of the EU Cybersecurity Act, cybersecurity as a *state*, a protective sphere in which natural and legal persons are (cyber)secure, came into place. By now the basic components necessary for birth of a new right are available: its addressees include potentially everybody active in the digital realm, and the same applies to its recipients. Its scope is to protect against "*cyber threats*", which are to be understood anything that could possibly "*damage, disrupt or adversely affect*" natural and legal persons.

Apparently, a lot more needs to be done for a new right to cybersecurity to fully emerge. Its exact content needs to be elaborated, perhaps choosing between the two available models at hand: either that of a detailed prescription or, in more traditional human rights style, by means of a simple relevant declaration. Similarly, the method through which to accomplish it will need to be decided, either by way of new specialised regulatory instrument, or amendment of a legal act currently in effect.

These steps are however necessary and important in view of the reasons that make an introduction of a new right to cybersecurity necessary. *Prima facie* this would constitute a necessary development, if the EU wishes for its resources and efforts in cybersecurity policy to bear fruit. If not accompanied by concrete legal rights and obligations even the most detailed cybersecurity policy risks being ignored by its addresses, who would unavoidably measure the cost of compliance against the legal risk of non-compliance. Nevertheless, this is not the most important reason why a new right to cybersecurity is needed in EU law. The main reason behind its introduction would be to empower individuals to defend themselves in the digital realm. A new right would give persons the necessary tools to protect themselves in the new digital reality and it would also require that their wishes are respected by others.

While doing so, the model of personal data protection could be of invaluable assistance. The two fields are inter-

[100] See Art. 1.1 of the 1995 EU Data Protection Directive.
[101] See Wessel R A, Cybersecurity in the European Union, supra, with further references.
[102] Wessel R A, European Law and Cyberspace, supra; See also Márton V, "5G Networks, (Cyber)Security Harmonisation and the Internal Market: the Limits of Article 114 TFEU", European Law Review, 2020, 45 (4).
[103] Art. 3.2 of the 1995 EU Data Protection Directive.
[104] See Art. 16 TFEU.

connected, being both at the forefront of affording protection against the risks posed by new technologies. Data protection preceded by far cybersecurity and by now benefits from a comprehensive legal framework at EU and Member State level. Its know-how could prove invaluable to cybersecurity. Most pertinently, it would help to address the two main objections against introduction of a new right to cybersecurity: EU competence, and its relationship with national and state security.

Cybersecurity still needs to find its proper place within the traditional notion of security. While security is a concern as ancient as humanity, cybersecurity is a relatively recent concept that is still in need of assessment and elaboration. A distinction between cybersecurity as *praxis* and as a *state* could perhaps assist understanding better. It also paves the way for introduction of a new relevant right. These approaches are not foreign to what has already taken place at EU law level; they form the necessary steps towards affording Europeans with the same level of security enjoyed in real-life as in the digital life – for at least as long as the two remain separate.

Declaration of Competing Interest

The authors declare no conflict of interest.

Data Availability

No data was used for the research described in the article.