Chapter 5
Cybersecurity Regulation in the European Union: The Digital, the Critical and Fundamental Rights

Gloria González Fuster and Lina Jasmontaite

Abstract This chapter provides an overview of the European Union (EU) policies and legislative measures developed in an attempt to regulate cybersecurity. By invoking a historical perspective, policy developments that have shaped the cybersecurity landscape of the EU are highlighted. More concretely, this contribution investigates how the EU has been delimiting and constructing its cybersecurity policies in relation to different and sometimes opposing objectives, and questions what such choices reveal about (and how they determine) the evolution of the EU's cybersecurity policy and its legal contours. For this purpose, the major steps in the evolution of the EU's agenda on cybersecurity are analysed, ranging from the adoption of the 2013 Cybersecurity Strategy to other numerous norms, initiatives and sectorial frameworks that tackle issues arising from the active use of information systems and networks. The chapter reviews the mobilisation of multiple areas (such as the regulation of electronic communications, critical infrastructures and cybercrime) in the name of cybersecurity imperatives, and explores how the operationalisation of such imperatives surfaced in the EU cybersecurity strategy published in September 2017. The chapter suggests that one of the key challenges of cybersecurity regulation is to impose the right obligations on the right actors, through the right instrument. Reflecting on issues surrounding the current liability framework dating from the 80s, it considers how principles such as data protection by design and default as well as the 'duty of care' have emerged. Finally, the chapter considers how the perception of cybersecurity's relationship with (national) security plays a determinant role in the current EU legislative and policy debates, where fundamental rights considerations, despite being acknowledged in numerous policy documents, are only considered in a limited manner.

Keywords Cybercrime · Cyberdefence · Cybersecurity · EU law

G. G. Fuster · L. Jasmontaite (✉)
Vrije Universiteit Brussel (VUB), Research Group on Law, Science, Technology and Society (LSTS), Brussels, Belgium
e-mail: gloria.gonzalez.fuster@vub.be; lina.jasmontaite@vub.be

M. Christen et al. (eds.), *The Ethics of Cybersecurity*, The International Library
of Ethics, Law and Technology 21,
https://doi.org/10.1007/978-3-030-29053-5_5

5.1 Formulating Cybersecurity as a Policy Area and Its Objectives

The publication of the First European Union (EU) Cybersecurity Strategy in 2013 marked the formal establishment of 'cybersecurity' as a new policy area in the EU (European Commission and High Representative 2013). This recognition was a long awaited development acknowledging the blurring of lines in three initially distinct but converging policy areas of (1) network and information security measures that target operators of essential services, and providers of critical and digital infrastructures; (2) electronic communications, including privacy and data protection issues; and (3) cybercrime (van der Meulen et al. 2015; Christou 2016). It took over 20 years for a gradually growing number of scattered initiatives addressing issues concerning the digital environment—ranging from digital signatures and ecommerce to cybercrime and critical infrastructure—to be recognised under an overarching umbrella term of cybersecurity. In addition, the area has, most recently included measures concerning cyberdefence (Christou 2016).

This chapter aims to capture the current state of the art of the cybersecurity landscape in the EU. It does so by analysing EU policies and legislative measures in an attempt to regulate cybersecurity; identifying the challenges of conceptualising this policy area; reflecting on the limitations imposed on cybersecurity regulation by the principle of conferral and the way this affects the choice of regulatory measures and addressees of regulation; and, finally, discussing the triggers shaping cybersecurity regulation, in particular political developments and the perception of EU values and interests.

It is now established that a highly fragmented legal framework constitutes the European cybersecurity policy area and that this area is bound to develop further given the EU's digital dependency. As suggested by Ramses Wessel, cybersecurity forms "an excellent example of an area in which the different policy fields need to be combined (a requirement for horizontal consistency), and where measures need to be taken at the level of both the EU and Member States (calling for vertical consistency)" (Wessel 2015: 405). Therefore, it is proposed that the five strategic EU cybersecurity priorities listed below capture the complexity of the policy area and provide insights into how both horizontal and vertical consistency could be attained. The five strategic EU cybersecurity priorities are (European Commission and High Representative 2013: 4–16):

- *Achieving 'cyber resilience'* by establishing minimum requirements for the functioning, cooperation and coordination of national competent authorities for network information systems.
- *Reducing cybercrime* by (a) ensuring a swift transposition of the cybercrime related EU Directives, (b) encouraging ratification of the Council of Europe's Budapest Convention on Cybercrime (Council of Europe 2001), and (c) funding programmes for the deployment of operational tools.

- *Developing cyberdefence policy and capabilities related to the Common Security and Defence Policy (CSDP)* by (a) assessing operational EU cyberdefence requirements, (b) developing the EU cyberdefence policy framework, (c) promoting dialogue and coordination between civilian and military actors in the EU, and (d) facilitating a dialogue with international partners.
- *Developing the industrial and technological resources for cybersecurity* by (a) establishing a public-private platform on Network and Information Security (NIS) solutions, (b) providing technical guidelines and recommendations for the adoption of NIS standards and good practices, and (c) encouraging the development of security standards for technology 'with stronger, embedded and user-friendly security features'.
- *Establishing a coherent international cyberspace policy for the EU and promoting core EU values* by mainstreaming cyberspace issues into EU external relations and Common Foreign and Security Policy (CFSP), and by supporting capacity building on cybersecurity and resilient information infrastructures in third countries. More specifically, the EU should ensure that its consultations with international partners on cyber issues are designed to complement the existing bilateral dialogues between the Member States and third countries. These consultations shall be driven by the EU core values of human dignity, freedom, democracy, equality, the rule of law and the respect for fundamental rights. Following the objectives of this priority, the EU aims to attain a high level of data protection, including the protection of personal data transferred to third countries.

In summary, the term 'cybersecurity', from an EU perspective, entails a combination of cyber resilience, cybercrime, cyberdefence, (strictly) cybersecurity and global cyberspace issues.

By identifying these five distinct priority areas, the 2013 Strategy aimed "*to make the EU's online environment the safest in the world*" (European Commission and High Representative 2013) —somehow challenging the cliché that no technical environment is 100% secure. It is hard to measure the current cybersecurity capacity at the EU level and whether it effectively results in *the safest* possible online environment. Two ransomware attacks known under the names of WannaCry and Petya (malware) that broke out in 2017 indicated that many improvements, in particular in terms of the response and cooperation among different actors concerned with cybersecurity at EU and national level, could still be made.

The two mentioned attacks are also interesting to consider from another perspective. They constitute a particularly good demonstration of a series of characteristics of cybersecurity as a policy area. First, this policy area recognises that cyber-attacks are the new reality and that such attacks not only can have cascading effects that are hard to predict and but that they may also cripple many more organisations in Europe than anticipated. At the same time, the recognition of the seriousness of cyber-attacks increases in the aftermath of cyber-incidents that inflict damage on EU-based businesses. Secondly, tackling cyber-attacks requires close cooperation between well-established networks composed of both public and private entities.

Thirdly, ineffective cybersecurity policies may obstruct the smooth functioning of the Digital Single Market, which in turn may have detrimental monetary implications for individuals, businesses and the public sector.

In autumn 2017, preceding the mentioned two cyber-attacks, the European Commission (EC) and the High Representative of the Union for Foreign Affairs and Security Policy published a Joint Communication to the European Parliament and the Council of the European Union titled *Resilience, Deterrence and Defence: Building strong cybersecurity for the EU* (the Second EU Cybersecurity Strategy or 2017 Joint Communication) which built on previous initiatives and sectorial frameworks, such as the legal frameworks for telecommunications, electronic commerce and electronic signatures, policy and regulatory measures, which have traditionally delineated the fragmented landscape of EU's approach to cybersecurity. The Second EU Cybersecurity Strategy emphasised the need for measures that would allow (1) building greater EU resilience to cyber-attacks, (2) facilitating detection of cyber-attacks, and (3) strengthening international cooperation on cybersecurity (European Commission and High Representative of the Union for Foreign Affairs and Security Policy 2017).

The 2017 Joint Communication illustrates well the evolution of the EU's understanding of the cybersecurity landscape. It also foresees that for the conventional idea of cybersecurity being a multi-stakeholder responsibility to be implemented in the EU, "multiple layers of government, economy and society should be involved" in order to improve cybersecurity capacity (European Commission and High Representative of the Union for Foreign Affairs and Security Policy 2017, 3). For this purpose, the Second EU Cybersecurity Strategy insists on having "more robust and effective structures to promote cybersecurity and to respond to cyber-attacks in the Member States but also in the EU's own institutions, agencies and bodies", which to some extent delineates the scope of the EU cybersecurity area (European Commission and High Representative of the Union for Foreign Affairs and Security Policy 2017: 3). Similarly important is the call for "a more comprehensive, cross-policy approach to building cyber-resilience and strategic autonomy, with a strong Single Market" which receives stronger emphasis in comparison with the First EU Cybersecurity Strategy (European Commission and High Representative of the Union for Foreign Affairs and Security Policy 2017: 3). The Second EU Cybersecurity Strategy, despite not being a legally binding instrument, also clarifies the roles of different EU agencies shaping the cybersecurity policy area.[1]

From a legal perspective, particularly relevant is the Second Cybersecurity Strategy's willingness to address liability questions in cybersecurity (European Commission and High Representative of the Union for Foreign Affairs and Security Policy 2017: 6). The Second EU Cybersecurity Strategy, following up on the Mid-Term Review on the implementation of the Digital Single Market Strategy which was published in spring 2017, highlights the need to analyse the implications of new

[1] In particular, the European Union Agency for Law Enforcement Cooperation (Europol), the European Union Agency for Law Enforcement Training (CEPOL) and the European Union Agency for Network and Information Security (ENISA) in the domain of cybersecurity.

technologies and to take steps to address the risks that they create. The Second EU Cybersecurity Strategy does not elaborate on such implications but instead relies on statements made in the Mid-Term Review—the high-level policy document representing positions of different units of the Commission working within this area. The Mid-Term Review refers to security challenges caused by Internet of Things (IoT) based applications, including "the *safety* of connected systems, products and services, as well as for businesses' liability" (EC 2017b: 11).[2] The Mid-Term Review explains that "[f]aulty sensors, vulnerable software or unstable connectivity may make it difficult to determine who is technically and legally responsible for any ensuing damage" (EC 2017b: 11). In this, the EC vows to revise the existing legal framework to address "new technological developments (including robotics, Artificial Intelligence and 3D printing), especially from the angle of civil law liability and to take into account the results of the ongoing evaluation of the Directive on liability for defective products and the Machinery Directive" (EC 2017b: 11).

The need to address liability in this context then resurfaces in the 2018 Communication on Artificial Intelligence, where it is highlighted that '[a]s with any transformative technology, some AI applications may raise new ethical and legal questions, for example related to liability' (EC 2018: 2). Liability was also referred to as a concern of cloud computing contracts (EC 2012). The frequency at which liability questions remerge in policy debates and documents suggests that it is a principled issue that requires legal consideration.

5.2 A Virtuous But Vicious Circle of Regulation: From Cybersecurity Law to Policy and Vice Versa

It is interesting to note that whereas the two EU Cybersecurity Strategies followed the adoption of numerous legislative measures concerning cybersecurity, they put forward policy objectives which subsequently resulted in legislation, namely the Network and Information Security Directive and the Cybersecurity Act, which further clarifies the role and mandate of the European Union Agency for Network and Information Security (ENISA). Building on this observation, we suggest that the cybersecurity area revives itself by both law and inter-area policy measures. Policy measures from various policy areas eventually led to changes and adjustments in various EU legal frameworks and *vice versa*. The following paragraphs provide two illustrative examples supporting this claim.

First, while the Second EU Cybersecurity Strategy proposes to set up an EU certification framework that would benefit both business and the users, the details over the envisioned certification framework that would "inform and reassure

[2] Whereas the word 'safety' at first glance may seem to be displaced and the term 'security' would have been a better fit, it reflects the very carefully selected language of the EC. The use of this term establishes a link with the General Product Safety Directive 2001/95/EC and The Radio Equipment Directive 2014/53/EU.

purchasers and users about the security properties of the products and services they buy and use" are provided in the proposal for a Cybersecurity Act (European Commission and High Representative of the Union for Foreign Affairs and Security Policy 2017: 5). This framework, though it would not result in "any immediate regulatory obligations", would allow certification and conformity self-assessment of ICT products and services.[3]

The mention of the 'duty of care' principle in the Second EU Cybersecurity Strategy is the second example, which reflects a vicious circle approach to cybersecurity regulation. Stakeholders are encouraged to explore this principle as it may lead to "a range of methods from design to testing and verification", which could potentially tackle and minimise software vulnerabilities (European Commission and High Representative of the Union for Foreign Affairs and Security Policy 2017: 5). The rationale of this principle was to a certain extent already pursued in the Network and Information Security Directive adopted in 2016—a year before the Second Cybersecurity Strategy was published. More specifically, the 'duty of care' principle is anchored in Article 14 of the NIS Directive, which obliges Member States to foresee security requirements and incident notification requirements for operators of essential services (e.g. providers of electricity or water). More specifically, entities that have been identified as operators of essential services by Member States have to take appropriate measures that would enable the prevention and minimisation of the "the impact of incidents affecting the security of the network and information systems used for the provision of such essential services, with a view to ensuring the continuity of those services" (European Parliament and Council of the European Union 2016: Article 14.2). The same provision also requires operators of essential services to notify as soon as reasonably possible "the competent authority or the CSIRT of incidents having a significant impact on the continuity of the essential services they provide" (European Parliament and Council of the European Union 2016: Article 14.3).

This section demonstrated that the cybersecurity area is evolving and comprised of highly fragmented measures. Cybersecurity is a horizontal problem, which is in a sense a common denominator of various new technologies connected to the World Wide Web. The following section illustrates some challenges and risks arising from the different perceptions of cybersecurity as a policy area.

5.3 Conceptualising Cybersecurity as a Policy Area Through Piecemeal Legislation and Policy

As mentioned, numerous policies and regulatory measures have been adopted to advance the security of citizens, businesses and public administrations in the areas of network and information security measures, electronic communications and

[3] The use of standards is generally promoted by the EC.

cybercrime. In fact, the EU has only recently started using the term 'cybersecurity' in its policy documents. We suggest that the adoption of a comprehensive EU Cybersecurity Strategy in 2013 can be considered the tipping point which triggered the increased use of the term in EU policy documents (e.g., in 2016 Communication 'Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry', and the Cybersecurity Act).

The 2013 Strategy provided in a footnote a definition according to which "[c] ybersecurity commonly refers to the safeguards and actions that can be used to protect the cyber domain, both in the civilian and military fields, from those threats that are associated with or that may harm its interdependent networks and information infrastructure" (European Commission and High Representative 2013: 3). In this context, cybersecurity's primary objectives were considered to be the preservation of "the availability and integrity of the networks and infrastructure and the confidentiality of the information contained therein" (European Commission and High Representative 2013: 3).

This definition, to a certain extent, deviated from a prior suggestion put forward by the European Network and Information Security Agency (ENISA). ENISA proposed using "a contextual definition" because cybersecurity is a broad and evolving term, arguing that whereas opting for a specific definition can allow for maintaining clarity, stakeholders and policy makers should select definitions that fit their particular needs in a specific context (ENISA 2016: 28). Consequently, various stakeholders and policy makers, including EU institutions, often opt for definitions developed by standardisation organisations, such as the European Committee for Electrotechnical Standardization (CENELEC) and the International Organization for Standardization (ISO), or international organisations, such as the International Telecommunication Union (ITU). Not surprisingly, by now numerous definitions coexist focusing on different dimensions of cybersecurity (e.g. political, military, economic, technical, legal and citizens').

Although some definitions may appear extremely broad,[4] narrow and more specific definitions, in particular related to technical requirements, might also need to be considered with caution. Whereas they may serve well during a negotiation phase, it is important to consider limitations embedded in them. For example, many definitions developed by standardisation organisations target the micro-management level. Therefore, they may carry a risk of conceptualising 'cybersecurity' in an unduly limited way. For example, cybersecurity may be seen only as a concern of risk that may arise online; it may be understood as a protection of only virtual assets; or it may only target malicious activities. Such definitions carry a risk of not considering, for instance, implications for individuals and their rights.

[4] For example, according to the ITU in Plenipotentiary Resolution 181 (Guadalajara, 2010) on definitions and terminology relating to building confidence and security in the use of information and communication technologies, consider cybersecurity to be "*the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets*".

Definitions used to refer to cybersecurity by various actors, including EU Member States, bodies and institutions, typically represent different perspectives, which can potentially be at odds with each other (see for an overview Table 5.1). For example, whereas ENISA often frames cybersecurity as a mere technical issue, some Member States in their national security strategies regard cybersecurity as an issue of national security (e.g. Estonia and Slovakia).

The possibility of attaching different meanings to the term 'cybersecurity' has both advantages and disadvantages. It indicates the flexibility of the term that can adapt to changing circumstances. At the same time, an ever-evolving term can become overly inclusive or broad in a manner that would obstruct coherent regulation in this area and in this way hamper the development of regulatory measures. It also opens a space for friction between EU and Member States powered around the national security notion. Consequently, this shifting meaning of the term may make progress in this particular policy area hard to attain, or at least less visible.

To render the conceptualisation of cybersecurity more complicated from a legal perspective, in measures addressed to the Member States, EU institutions appear to be reluctant to even use the term. That is the case, for example, of the EU adopted 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 (NIS Directive). The NIS Directive lays down obligations for all Member States to adopt certain measures (e.g. national strategies on the security of network and information systems) that would enable the development of a culture of security across industries and sectors that rely on the use of information communication technologies.

Within the context of this Directive, "security of network and information systems" is regarded as "the ability of network and information systems to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those network and information systems" (European Parliament and Council of the European Union 2016 Article 4 (2)). This definition seems to align with the conception reflected in the EU Cybersecurity Strategy, where the underlying objective of cybersecurity is considered to be the preservation of "the availability and integrity of the networks and infrastructure and the confidentiality of the information contained therein" (European Commission and High Representative 2013: 3). Nonetheless, the NIS Directive formally addresses "security of information systems and networks", and not cybersecurity.

In short, the ambiguity embedded in and sustained by the term 'cybersecurity' allows for the term to be invoked across the different policy areas mentioned above. Whereas this is not problematic in itself, the fragmented approach may not be cost-efficient (ENISA 2017: 4). More importantly, it begs the question of whether EU cybersecurity shall be considered an autonomous notion, with a specific nature in EU policy as opposed to other policy levels.

Table 5.1 Definitions of cybersecurity in national cybersecurity strategies of EU Member States

Document title, country, year	Definition
Austrian Cyber Security Strategy, 2013	The term 'cyber security' stands for the security of infrastructure in cyber space, of the data exchanged in cyber space and above all of the people using cyber space.
Croatian Cybersecurity Strategy, 2015	Cyber security encompasses activities and measures for achieving the confidentiality, integrity and availability of information and systems in cyberspace.
Czech Republic Cybersecurity Strategy for the period of 2015–2020	Cyber security comprises a sum of organisational, political, legal, technical, and educational measures and tools aiming to provide a secure, protected, and resilient cyberspace in the Czech Republic for the benefit of both public and private sectors, as well as for the general public.
Cybersecurity Strategy of the Republic of Cyprus: Network and Information Security and Protection of Critical Information Infrastructures, 2012	Cybersecurity refers to the broader security of networked systems that operate in cyberspace, i.e. in most cases connected to the internet, and this term also covers the safe and secure usage of these systems by end users.
Dutch National Cyber Security: Strategy from awareness to capability, 2018	Cyber security is the entirety of measures to prevent damage caused by disruption, failure or misuse of ICT and how to recover should damage occur.
Estonian Cyber Security Strategy, 2014–2017	Cyber security is an integral part of national security; it supports the functioning of the state and society, the competitiveness of the economy and innovation.
Finland's Cyber security Strategy, 2013	Cyber security means the desired end state in which the cyber domain is reliable and in which its functioning is ensured.
Italian National Strategic Framework for Cyberspace Security, 2013	With the term cyberspace, we refer to the complex of all interconnected ICT hardware and software infrastructure, to all data stored in and transferred through the networks and all connected users, as well as to all logical connections however established among them. It therefore encompasses the internet and all communication cables, networks and connections that support information and data processing, including all mobile internet devices.
Cyber Security Strategy for Germany, 2011	Cyberspace is the virtual space of all IT systems linked at data level on a global scale. The basis for cyberspace is the internet as a universal and publicly accessible connection and transport network, which can be complemented and further expanded by any number of additional data networks. IT systems in an isolated virtual space are not part of cyberspace.
Hungarian Government Decision No. 1139/2013 (21 March) on the National Cyber Security Strategy of Hungary, 2013	Cyber security is the continuous and planned taking of political, legal, economic, educational, awareness-raising and technical measures to manage risks in cyberspace that transforms the cyberspace into a reliable environment for the smooth functioning and operation of societal and economic processes by ensuring an acceptable level of risks in cyberspace.

(continued)

Table 5.1 (continued)

Document title, country, year	Definition
Cyber Security Strategy of Latvia, 2014–2018	Cyber security is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organisation and user's assets. Organisation and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment.
Lithuanian Cyber Security Strategy, 2011–2019	Electronic information security equates to cyber security.
Luxembourg Cybersecurity Strategy, 2015	Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organisation and user assets. Organisation and user assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organisation and user assets against relevant security risks in the cyber environment.
Malta, National Cyber Security Strategy, Green Paper, 2015	Cybersecurity "is the safeguards and actions that can be used to protect cyber domain from those threats that are associated with or that may harm its interdependent networks and information infrastructure. It strives to preserve the availability and integrity of the networks and infrastructure and the confidentiality of the information contained therein."
Cyberspace Protection Policy of the Republic of Poland, 2013	Cyberspace security—a set of organisational and legal, technical, physical and educational projects aimed at ensuring the uninterrupted functioning of cyberspace.
Cyber Security Concept of the Slovak Republic for 2015–2020	Cyber security is one of the defining elements of the security environment of the Slovak Republic and a subsystem of national security. At a state level, it is a system of continuous and planned increasing of political, legal, economic, security, defence and educational awareness, also including the efficiency of adopted and applied risk control measures of a technical-organisational nature in cyber space in order to transform it into a trustworthy environment providing for the secure operation of social and economic processes at an acceptable level of risks in cyber space.
National Cyber Security Strategy of Spain, 2013	Cyber security is a necessity of our society and our economic model.
UK National Cyber Security Strategy, 2016–2021	'Cyber security' refers to the protection of information systems (hardware, software and associated infrastructure), the data on them and the services they provide from unauthorised access, harm or misuse. This includes harm caused intentionally by the operator of the system or accidentally, as a result of failing to follow security procedures.

5.4 Principle of Conferral Limits the Scope of Cybersecurity

Cybersecurity is nowadays typically regarded as a highly complex issue which requires the active involvement of a range of stakeholders, including the legislator. It is commonly agreed that the legislator is in particular responsible for setting up an appropriate regulatory framework within which private and public entities could carry out their tasks and duties (Bannelier and Christakis 2017; see also Chap. 10). This is a significant change from an initial understanding of cybersecurity according to which it was perceived as a purely technical matter related to measures ensuring the availability, integrity and confidentiality of information and information systems (see Chap. 2).

When discussing cybersecurity regulation in the EU, it is necessary to consider the principle of conferral. Whereas in general the EU can legislate in areas where it is more appropriate than for the Member States to act individually, introducing any regulatory measure at the EU level, including measures concerning cybersecurity, requires the legislator to provide legal justification: in other words a legal basis (Wessel 2015). In particular, the proposal for a legislative measure has to meet the criteria set out in Article 5 of the Treaty of the EU (TEU). In principle, this means that to establish competence over a policy area, a legislative measure has to fall under one of these two situations: (1) either “the proposed action cannot be sufficiently achieved by the Member States, either at central level or at regional and local level” or (2) “by reason of the scale or effects of the proposed action, be better achieved at Union level” (TEU; Article 5(3)).

Considering the principle of conferral and in particular the limited competences of the EU in security issues, the EC was obliged to provide an explanation for acquiring competence to legislate in the cybersecurity area. This occurred in the NIS Directive by establishing a link between cybersecurity and the internal market, largely resembling the reasoning used in order to introduce rules for personal data protection in 1995 (González Fuster 2014: 125). Recital 5 of the NIS Directive proclaims that the diverse Member States’ practices with regards to cybersecurity measures hinder the protection awarded to consumers and business, and consequently reduce “the overall level of security of network and information systems” (European Parliament and Council of the European Union 2016). The NIS Directive was adopted to increase consistency of Member States’ practices concerning cybersecurity measures.

5.5 Remaining Challenges to an Effective Cybersecurity Legal Framework

Different actors, including academics, policy makers and private sector representatives try to get their heads around the cybersecurity area in the EU. To ease such tasks, the European Court of Auditors, an institution that takes care of EU tax payers' interests, published a report providing an excellent overview of the EU's complicated cybersecurity policy framework. The report identifies many challenges to effective policy delivery, such as the meaningful evaluation and accountability of policy and legislative framework; addressing gaps in EU law and its uneven transposition; aligning investment levels with goals; the need for a clear overview of EU budget spending; adequately resourcing the EU's agencies; and strengthening information security governance, and threat and risk assessments (European Court of Auditors 2019).

5.5.1 Choice of Appropriate Regulatory Measures

Most legal measures concerning cybersecurity are found in directives that are minimal harmonisation measures (e.g. NIS Directive and Directive on Attacks against Information Systems). In practice, this means that Member States are free to choose the form and methods to implement requirements stemming from such directives. This flexibility may be seen as a weakness of minimal harmonisation tools. However, directives are considered to be the best tool when introducing a complex legislative change, such as the introduction of a new regulatory area (Craig and de Burca 2015: 106).

In some areas that have been traditionally more strictly regulated, such as the protection of personal data and health care, there is a tendency to adopt more harmonised regulation (see also Chaps. 7 and 17). Examples include the General Data Protection Regulation (GDPR), repealing Data Protection Directive 95/46/EC and Medical Device Regulation (MDR) repealing the Directive on Medical Devices (European Union 2016: 2017).

The MDR is particularly interesting as it aims to establish a "predictable and sustainable regulatory framework for medical devices which ensures a high level of safety and health whilst supporting innovation" (European Union 2017, Recital 1). The MDR defines a 'medical device' as "any instrument, apparatus, appliance, *software*, implant, reagent, material or other article intended by the manufacturer to be used, alone or in combination, for human beings for one or more of the following specific medical purposes" (European Union 2017, Article 2.1). Such purposes may include the diagnosis, prevention, monitoring, prediction, prognosis, treatment or alleviation of disease. The term 'software' is not a new addition to this definition, and it can be found in the Directive on Medical Devices. However, the use of this term means that apps and their accessories that are developed for a medical purpose (e.g. monitoring and measuring blood pressure for diabetes management) are subject to rules as well as safety and performance requirements listed in this regulation, including a comprehensive post-market surveillance system. However, qualifying some software, such as mobile apps, as a medical device is sometimes particularly challenging. A wafer-thin line separates health and well-being apps that are considered to be medical devices from apps that are not considered to be so.

5.5.2 *Targeting the Right Addressees*

Cybersecurity measures at the EU level target different actors. Consequently, there are numerous addressees of legislative measures. For example, recent regulatory measures, such as the GDPR and NIS Directive, impose requirements on the ones responsible for the certain operations, namely controllers, processors, providers of essential services and providers of digital infrastructure. They all must take appropriate security measures in response to the risk that they may be subjected to.[5]

The fact that the current regulation of data protection by design focuses exclusively on data controllers (i.e., entities defining the means of the processing of personal data), however, is regrettable, as it can address only part of the problems in the area. The obligation to implement data protection by design does not extend to the actual developers of technology or service providers (Jasmontaite et al. 2018: 173). Recital 78 of the GDPR reveals some hesitations of the legislator, noting that not only controllers but also processors, producers of the products, services and applications, should be among the ones who should consider the right to data protection when developing and designing products, services and applications based on the processing of personal data. While recognising the limited legal value of this Recital (i.e. it is not legally binding but helps in the interpretation Article 25 of the GDPR), the actual software developers or producers of hardware, unless they are data controllers or processors, are de facto not subjected to the legal obligations foreseen in the EU data protection framework.

The debate within the field of data protection over who should be responsible for ensuring the rights of individuals in the online environment is, as a matter of fact, still an open matter in the EU. Discussions concerning the proposed ePrivacy Regulation also confirm that this is an unresolved issue. This being said, it may be concluded that one of the key challenges of cybersecurity regulation is to impose the right obligations on the right actors, through the right instrument—in addition to avoiding the imposition, through disparate instruments, of very similar but not exactly coincidental obligations on the same actors. For example, it is estimated that at the moment there are "at least eleven instruments of EU law having a bearing on [data and information security] breaches, five in the Area of Freedom, Security and Justice (AFSJ) and six in the internal market" (Porcedda 2018, 3).

The issue of targeting the relevant actors is also a pressing one in discussions surrounding the EU liability framework (Directive 85/374/EEC), which in many cases may inappropriately favour some software developers. Whereas software is not explicitly included under the scope of the Product Liability Directive, the academic doctrine has argued that, for the purposes of product liability, software should be perceived as a product (Alheit 2001: 194). According to Article 3 of the Product Liability Directive, which has been transposed into national laws, any person in the supply chain can be held liable and requested to compensate victims

[5] See Articles 25.1 and 32 of the GDPR and Articles 14 and 16 of the NIS Directive.

for any personal injury or damage caused to private property caused wholly or in part by a defect of a product. In such cases, the plaintiff does not have to prove negligence on the part of the producer, but only that it is was defective and the damage occurred because there was causality between the defect and damage (Alheit 2001, 197–99).

This means in practice that the EU has opted in for a strict liability regime for which no proof of fault is necessary. At the same time, it should be noted that in circumstances where a product leads to a pure economic loss or infringement of individuals' rights, the strict liability regime may not be invoked, as the damage should occur to a person or to a private property. Furthermore, the Product Liability Directive in Article 7 foresees that there are several situations in which the producer's liability can be avoided. Recognising the limitations of the current liability framework, the European Parliament noted that in the context of the IoT "tightening up liability regimes" would be desirable as it could "lead to a better quality of products and a more secure environment" (European Parliament 2017: 13).

A new approach to the liability framework could provide individuals with the comprehensive and meaningful protection of their security, including the protection of their personal data (Daley 2016). Such an approach, as proposed by Daley, would require to balance ex ante incentives to invest in security with ex post liability, incentivise software developers to publicly disclose source code, and promote trust and public confidence in embedded systems (Daley 2016). It seems that this approach, though controversial, could help to develop the "high-quality, affordable, interoperable and trustworthy cybersecurity products" that the EC called for in June 2017 (Speech by Vice-President Ansip 2017).

5.5.3 The Long-Awaited Recast of Product Liability Directive, Pending

As discussed above, it is generally assumed that clearly defined liability framework for devices, applications and services could improve the protection of individuals and consequently that of the cyberspace. However, the current liability framework dates back from the 1980s and does not address such complex issues as embedded systems, embedded software and application software. It seems that there is a common understanding and agreement that regulating software and including it into the framework of Council Directive 85/374/EEC concerning liability for defective products would represent a major milestone. This would clarify the current standing of software that is perceived differently across Member States, both as a service and as a product.

In spite of this, it seems that these questions will remain unaddressed for the time being. In this context, the EC is promoting the use of code of conducts and preparing interpretative guidance of the Liability Directive.[6] In light of the policy line taken by the EC, which does envision the recast of the Liability Directive, it comes as no surprise that the European Parliament might look for alternative legal clarification of the current legal vacuum via other legislative proposals. For example, in its amendments on the proposal for a directive of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content, the European Parliament proposed specific rules for software that is embedded in tangible goods (smart goods). Although such 'isolationism' may be welcome, it may create fragmentation in the regulatory landscape, without necessarily improving an overall security of IT.

5.6 A Pressing Need to (Cyber)Secure EU Values and Interests

The observation that the "information revolution makes security an increasingly important concern in all sectors of society" has surely withstood the test of time and accurately reflects the current debates within the EU (Eriksson and Giacomello 2006). In a reflection paper on the future of cybersecurity regulation published in 2017, the EC emphasised the need to protect European values and interests against new types of threats (EC 2017c: 6). To improve the competitiveness and security of the EU, the reflection paper considered three scenarios (i.e. Security and Defence Cooperation, Shared Security and Defence, Common Defence and Security) which would allow Member States' industrial and technical resources to be pooled. Within the scope of that document, the EC questioned EU competence in the field of cybersecurity and considered ways to extend them beyond the limits of Digital Single Market. Cybersecurity becomes thus intertwined with the objectives of a Security and Defence Union and it is suggested that deeper integration, in particular the creation of a Common Defence Security, would improve cybersecurity resilience both at national and EU levels. It is also argued that a deeper integration scenario would allow for "Europe […] to deploy detection and offensive cyber-capabilities", which could be used in case of "cyber-attacks or external interference in Member States' democratic processes" (EC 2017c: 14–15).

The EC's rhetoric in recent policy documents could be regarded as favouring the consolidation of a broadened vision of cybersecurity through the specific prism of EU cybersecurity. It insists on the need for more cooperation and coordination of programmes concerning the interoperability of information systems for security, border and migration management. For example, the EC in one of its recent documents refers to 'the global cyberattack using ransomware' (known as WannaCry) as

[6] See, Commission publishes evaluation reports on EU rules on machinery safety and product liability, available at: https://ec.europa.eu/growth/content/commission-publishes-evaluation-reports-eu-rules-machinery-safety-and-product-liability_en, last accessed 15 November 2018.

a case demonstrating the need for expansion of EU actions, and thus acclaiming competence, within the cybersecurity domain (EC 2017a: 2). In another policy document, the EC relies on statistics about ransomware from the United States in order to strengthen its claim about the potential risks of cyberattacks for business, economy and democracy in the EU: "wider instruments for European solidarity and mutual assistance" in the field of cybersecurity could address these risks (EC 2017b: 12). This somehow far-stretched rhetoric could be in conflict with the rationale of EU better regulation policy, which should be driven by the "best available evidence" and the involvement of stakeholders (EC 2015: 5).

It is also possible to argue that the European Union could have taken a different approach in response to the increasing number of cyberattacks and cyberthreats. For example, Wojciech Wiewiórowski, Assistant EDPS, suggested that if appropriate security measures, required under data protection law, had been implemented, the mentioned attacks could have been prevented (Wiewiórowski 2017). This observation suggests that in response to cyberthreats, the European Commission may also emphasise the need for better implementation of requirements stemming from the existing EU data protection framework rather than the need for stronger cooperation mechanisms among concerned actors.

5.7 Concluding Remarks

The future of cybersecurity regulation appears to be at a crossroads: perceived cyber threats may shape political choices and lead to deeper integration, in particular with the ongoing discussions about the mandate of ENISA and the implementation of the Cybersecurity Act. As such, EU cybersecurity might actually have been at multiple crossroads since its inception.

This chapter aimed to reflect the particular challenges related to understanding cybersecurity regulation in the EU, based on a discussion of how such policy territory has been constructed. As outlined, numerous policy areas fall under the overarching scope of cybersecurity, and cybersecurity 'as such' is considered a horizontal issue. At the same time, the interconnected policy areas (e.g. cybercrime, IoT, autonomous vehicles, Artificial Intelligence, cloud computing) reflect and address a limited subset of cyber threats, ranging from the fight against cybercrime to the security of critical infrastructures and goods.

The EU cybersecurity landscape is continuously evolving as policy measures eventually lead to changes and adjustments in the legal framework and vice versa. The contours of this landscape have also been changing thanks to the flexibility, if not ambiguity, embedded in the very term 'cybersecurity', which entails both advantages and disadvantages. It may allow the area to integrate new technologies and policy issues as they emerge, but at the same time it can make it overly inclusive, potentially hindering the impact of regulation in this area.

When considering specific regulatory challenges, the current legal setup renders it, in a way, more difficult to impose the appropriate obligations on the right actors who could make a tangible contribution to the security of digital environments. This argument is illustrated by examples stemming from the GDPR, which does not formally address actual software developers or producers of hardware as such, unless they would qualify as data controllers or processors, and to the extent they would. The debate over who should be responsible for ensuring the rights of individuals and the security of their data as well, as well as that of any product and service connected to the online environment is, as a matter of fact, still ongoing in the EU and globally.

Emerging legal solutions for current uncertainty surrounding cybersecurity regulation might be regarded as encompassing the 'duty of care' principle, as well as the revision of the existing liability framework. However, considering the reluctance of the EC to revise the liability framework and address technical and legal riddles such as the regulation of liability of self-evolving software (i.e. Artificial Intelligence), it seems that it might be easier to introduce new principles.

Ultimately, the elastic nature of EU cybersecurity triggers questions regarding its relation to fundamental rights protection. EU cybersecurity policy seems to intermittently be *about* the protection of fundamental rights, sometimes about security *in accordance with* fundamental rights requirements, and occasionally about (almost any) cyber issues *independently from* fundamental rights considerations. A clarification of the—certainly profound—linkages between the effective regulation of cyber resilience, cybercrime, cyberdefence, (strictly) cybersecurity and global cyberspace issues would surely contribute to a more precise delineation of the necessary, albeit moving, boundaries of EU cybersecurity.

Acknowledgements The chapter was created with funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 700540.

References

Alheit K (2001) The applicability of the EU product liability directive to software. Comp Int Law J South Afr 34(2):188–209

Bannelier K, Christakis T (2017) Cyber-attacks – prevention-reactions: the role of states and private actors

Christou G (2016) Cybersecurity in the European Union: resilience and adaptability in governance policy, New Security Challenges Series. Palgrave Macmillan UK, London. https://doi.org/10.1080/09662839.2016.1160892

Council of Europe (2001) Convention on cybercrime, ETS no.185, Budapest. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185. Last access July 7 2019

Craig P, de Burca G (2015) EU law: text, cases and materials. Oxford University Press. https://doi.org/10.1093/he/9780198714927.001.0001

Daley J (2016) Insecure software is eating the world: promoting cybersecurity in an age of ubiquitous software-embedded systems. Stanf Tech Law Rev 19(3). https://law.stanford.edu/

publications/insecure-software-is-eating-the-world-promoting-cybersecurity-in-an-age-of-ubiquitous-software-embedded-systems/. Last access 7 July 2019

ENISA (2016) Definition of cybersecurity: gaps and overlaps in standardization

ENISA (2017) Principles and opportunities for a renewed EU cyber security strategy

Eriksson J, Giacomello G (2006) The information revolution, security, and international relations: (IR) relevant theory? Int Polit Sci Rev 27(3):221–244. https://doi.org/10.1177/0192512106064462

European Commission (2012) Communication on unleashing the potential of cloud computing in Europe, COM (2012) 529

European Commission (2015) Commission staff working document, better regulation guidelines, SWD (2015) 111 Final. Strasbourg

European Commission (2017a) Communication on Seventh Progress Report towards an Effective and Genuine Security Union, COM (2017) 261 Final

European Commission (2017b) Communication on the mid-term review on the implementation of the digital single market strategy: a connected digital single market for all. COM (2017) 228 Final. COM (2017) 228 Final. http://eur-lex.europa.eu/resource.html?uri=cellar:a4215207-362b-11e7-a08e-01aa75ed71a1.0001.02/DOC_1&format=PDF. Last access 7 July 2019

European Commission (2017c) Reflection paper on the future of European Defence

European Commission (2018) Communication on Artificial Intelligence for Europe, COM (2018) 237 Final

European Commission, and High Representative (2013) Cybersecurity strategy of the European Union: an open, safe and secure cyberspace

European Commission, and High Representative of the Union for Foreign Affairs and Security Policy (2017) Resilience, deterrence and defence: building strong cybersecurity for the EU. Joint Communication to the European Parliament and the council. https://doi.org/10.1016/j.neuint.2009.06.008

European Court of Auditors (2019) Challenges to effective EU cybersecurity policy. https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_EN.pdf. Last access 7 July 2019

European Parliament (2017) Report on the fight against cybercrime, motion for a resolution. http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A8-2017-0272+0+DOC+XML+V0//EN&language=en. Last access 7 July 2019

European Parliament, and Council of the European Union (2016) Directive (EU) 2016/1148 of the European Parliament and of the council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the union. Off J Eur Union Vol. L 194/1. https://doi.org/10.1017/CBO9781107415324.004

European Union (2016) Regulation (EU) 2016/679 of the European Parliament and of the council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46/ EC (GDPR). Off J Eur Communities https://doi.org/http://eur-lex.europa.eu/pri/en/oj/dat/2003/l_285/l_28520031101en00330037.pdf (last access July 7 2019)

European Union (2017) Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on Medical Devices, Amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and Repealing Council Directives 90/385/EEC and 93/42/EE. Off J Eur Union https://doi.org/http://data.europa.eu/eli/reg/2017/746/oj

González Fuster G (2014) The emergence of personal data protection as a fundamental right of the EU, Law, governance and technology series. Springer, Cham. https://doi.org/10.1007/978-3-319-05023-2

Jasmontaite L, Kamara I, Zanfir-Fortuna G et al (2018) Data protection by design and by default: framing guiding principles into legal obligations in the GDPR. European data protection law review 4(2). Lexxion Publisher: 168–89. https://doi.org/10.21552/edpl/2018/2/7

Porcedda MG (2018) Patching the patchwork: appraising the EU regulatory framework on cyber security breaches. Comput Law Secur Rev 000 Elsevier Ltd:1–22. https://doi.org/10.1016/j.clsr.2018.04.009

Treaty of Lisbon Amending the Treaty on European Union (TEU) (2007) Off J Eur Union:1–272

van der Meulen N, Eun AJ, Soesanto S (2015) Cybersecurity in the European Union and beyond: exploring the threats and policy responses. http://www.europarl.europa.eu/RegData/etudes/STUD/2015/536470/IPOL_STU(2015)536470_EN.pdf. Last access 7 July 2019

Vice-President Ansip (2017) The Chatham house annual cyber conference: evolving norms, improving harmonisation and building resilience. Speech by Vice-President Ansip

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

Wiewiórowski W (2017) Privacy, security and technology: the annual privacy forum 2017