International Review of Law, Computers & Technology

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/cirl20

The IoT and the new EU cybersecurity regulatory landscape

Pier Giorgio Chiara

To cite this article: Pier Giorgio Chiara (2022): The IoT and the new EU cybersecurity regulatory landscape, International Review of Law, Computers & Technology, DOI: 10.1080/13600869.2022.2060468

To link to this article: https://doi.org/10.1080/13600869.2022.2060468

Published online: 07 May 2022.

INTERNATIONAL REVIEW OF LAW, COMPUTERS & TECHNOLOGY
https://doi.org/10.1080/13600869.2022.2060468

OPEN ACCESS

The IoT and the new EU cybersecurity regulatory landscape

Pier Giorgio Chiara[a,b]

[a]Department of Law, University of Luxembourg, Luxembourg, Luxembourg; [b]Department of Law, University of Bologna, Bologna, Italy

ABSTRACT

This article aims to cast light on how the fast-evolving European cybersecurity regulatory framework would impact the Internet of Things (IoT) domain. The legal analysis investigates whether and to what extent existing and proposed sectoral EU legislation addresses the manifold challenges in securing IoT and its supply chain. It firstly takes into account the Cybersecurity Act, being the most recent and relevant EU legal act covering ICT products and cybersecurity services. Then, EU product legislation is scrutinised. The analysis focuses on the delegated act recently adopted by the Commission under the Radio Equipment Directive (RED), strengthening wireless devices' cybersecurity, the Medical Devices Regulation, the Proposal for a General Product Safety Regulation and the Proposal for a Machinery Regulation. Lastly, the proposal for a revised Network and Information Systems Directive (NIS2) is assessed in terms of its potential impact on the field of IoT cybersecurity. Against this backdrop, the article concludes by advocating the need for a separate horizontal legislation on cybersecurity for connected products. To avoid fragmentation of the EU's Single Market, a horizontal legal act should be based on the principles of the New Legislative Framework, with ex-ante and ex-post cybersecurity requirements for all IoT sectors and products categories.

ARTICLE HISTORY
Received 18 October 2021
Accepted 21 December 2021

KEYWORDS
IoT; cybersecurity; EU law

1. Introduction

Everyday objects around us increasingly collect huge amounts of data through connected sensors. These data are stored and processed either at the device level (e.g. edge computing) or in cloud service platforms. They are then shared with other devices and parties. This *network of things*,[1] embedded with software intelligence, sensors, and ubiquitous connectivity to the Internet (Rayes and Salam 2019, 2) is the Internet of Things (IoT). The IoT paradigm is of paramount importance for our societies since its application is wide-ranging and relate to home appliances, industry, transport systems, the health sector, the energy sector and, more broadly, smart cities. But not all connected devices can handle data collection, processing and transfers with equal security standards.

CONTACT Pier Giorgio Chiara piergiorgio.chiara@uni.lu Department of Law, University of Luxembourg, 4 Rue Alphonse Weicker, 2721 Luxemburg, Luxembourg; CIRSFID-ALMA AI, University of Bologna, Via Galliera 3, 40121 Bologna, Italy

Indeed, the IoT combines devices with limited central processing unit (CPU), memory and processing power (e.g. pressure sensors) (Bormann, Ersue, and Keranen 2014, 3) and devices with powerful processors, large memory and replenishable sources of energy. Less powerful devices, which are commonly referred to as resource-constrained (Cheruvu et al. 2020, 11), may not have adequate processing and storage capacity to embed security software or to perform techniques such as cryptography and pseudonymisation (European Union Agency for Fundamental Rights 2018, 409). These applications require low-cost hardware to be economically feasible, and they need to be small (Stapko 2008, 85). As the Internet of Things proliferates, enforceable rules require strengthening, to improve systems robustness and to ensure overall resilience and incident response capacities of public and private entities.

Against the backdrop of increasingly more unsecure devices in the Single Market (Giovanni and Silva 2018, 5; Wavestone 2021, 64–65) and threats to individual and collective (cyber)security and safety (Denardis 2020, 93–132) – with impacts on privacy and personal data protection (Chiara 2021), this contribution investigates to what extent existing and proposed EU legal frameworks applicable to IoT cybersecurity do or should impose cybersecurity requirements on the manufacturers of IoT products. To do so, two main research questions ought to guide the legal analysis: to what extent does the selected legislation take into account IoT cybersecurity? What are the manufacturers' obligations in relation to IoT cybersecurity?

The remainder of the article is organised as follows: section 2 investigates the EU cybersecurity certification framework for ICT products and services as introduced by Regulation 2019/881 (hereinafter, the Cybersecurity Act). Section 3 delves into the revision process of EU product legislation and looks how the cybersecurity of connected devices is considered. Different legal acts are under scrutiny: the Radio Equipment Directive and its delegated act – recently adopted by the EU Commission, the Medical Devices Regulation, the Proposal for a General Product Safety Regulation and the Proposal for a Machinery Regulation. Section 4 analyses the Proposal for NIS2 to investigate whether the revised Directive would cover more comprehensively the IoT than the current NIS Directive. Lastly, section 5 sketches some conclusive remarks on current policy discussions on the horizontal legislation on cybersecurity for connected devices.

2. The Cybersecurity Act and the IoT

The course of action proposed by the Commission in the second Cybersecurity Strategy of 2017 (European Commission 2017) resulted in Regulation (EU) 2019/881,[2] that is, the 'Cybersecurity Act'. For the first time, an EU piece of legislation defines 'cybersecurity': 'cybersecurity means the activities necessary to protect network and information systems, *the users of such systems and other persons affected by cyber threats* [emphasis added]'.[3] This conceptualisation differs substantially from the one enshrined in the Cybersecurity Strategy of 2013 (European Commission 2013). Whereas the first Strategy 'restricted' the concept of cybersecurity to the so-called CIA (i.e. confidentiality, availability and integrity) triad, the cornerstone of computer and information security, the broadened vision of cybersecurity (Fuster and Jasmontaite 2020, 111) includes *any persons,* and arguably their fundamental rights, that may be affected by cyber threats, going above and beyond the network and information systems dependency of the

2013 definition. The new Cybersecurity Strategy for the Digital Decade (later addressed in Section 4) echoes and deepens such reading, as it acknowledges that improving cybersecurity is essential, on the one hand, to trust and benefit from innovation, connectivity and automation; on the other hand, for safeguarding fundamental rights and freedoms, including the rights to privacy and to the protection of personal data, and the freedom of expression and information (European Commission and the High Representative of the Union for Foreign Affairs and Security Policy 2020).

The Cybersecurity Act is divided into two main parts. The first, from articles 3–45, strengthens the EU Agency on cybersecurity (ENISA), by granting it a permanent mandate,[4] more resources and new objectives[5] and tasks[6] in defending the digital ecosystem of the Union.[7] Against the background of a changed and rapidly evolving landscape, the Agency will 'act as a reference point for advice and expertise on cybersecurity for Union institutions, bodies, offices and agencies as well as for other relevant Union stakeholders'.[8] This regulatory step contributes to the paradigm shift in the EU institutional landscape described as 'agencification':

> EU agencies – like ENISA - are also increasingly authors of standards to be used in implementation of EU law by Member States. These roles of agencies have developed next to and alongside the more 'traditional' approach of regulatory law which consists of references to 'outside' standards set by private and semi-private standardisation bodies and scientific expertise. (Hofmann 2016, 13)

The second part, from articles 46–65, establishes the European cybersecurity certification legal framework. The European cybersecurity certification framework should serve a twofold purpose: it should (i) increase trust in ICT products, services and processes that have been certified under European cybersecurity certification schemes (ECCS) and, (ii) avoid the multiplication of conflicting or overlapping national cybersecurity certification schemes and thus reduce costs for undertakings operating in the digital single market.[9]

As regards the question of whether the Cybersecurity Act's scope encompasses the IoT, Article 2 defines an 'ICT product' as 'an element or a group of elements of a network or information system',[10] and an 'ICT service' as a service 'consisting fully or mainly in the transmission, storing, retrieving or processing of information by means of network and information systems'.[11] Following the understanding of IoT provided in the Introduction section of this article, it can be concluded that, at the same time, ICT products and services are indeed part of an IoT system and IoT devices are a subset of ICT products. Moreover, several recitals of the Cybersecurity Act explicitly mention the IoT (Hessel and Rebmann 2020, 32). In particular, recital 2 considers that the insufficient adoption of the principle of 'security by design' hinders IoT cybersecurity: in this respect, the limited use of certification schemes contributes to information asymmetries underlying the insufficient understanding of consumers vis-à-vis the overall security of ICT products, processes and services.[12]

Thus, the Regulation relies on the assumption that the full realisation of a secure Digital Single Market may be hindered by a lack of trust in the cybersecurity level of ICT products, services and processes,[13] due to insufficient information about the security features of such solutions. Without entering an epistemic discussion on the meaning of 'trust' (Durante 2021, 29–30), in less problematic terms it can be assumed that 'trust', here, refers to the (successful) delegation to third parties, whether national cybersecurity certification authorities,[14] conformity assessment bodies[15] or manufacturers themselves,[16] of the conformity evaluation procedure for evaluating whether specified requirements relating to an ICT product, ICT service or ICT process have been fulfilled. In other words, the certification mechanism is a means to enhance consumers' trust through a proof of conformity with specified cybersecurity thresholds, the 'assurance levels' ('basic', 'substantial' or 'high') which reflect the risk-based approach (Mantelero et al. 2021) of the Cybersecurity Act. It follows that trust, in the certification context, is associated with transparency (Kamara 2021, 98–99; Spagnuelo, Ferreira, and Lenzini 2019; Stahl and Strausz 2017); or, rather, the latter is a proxy for the former.

From a substantive legal standpoint, the Cybersecurity Act lays down cybersecurity certifications' minimum content and objectives. The Regulation provides for a detailed, non-exhaustive list of yet necessary elements that the schemes must contain, such as the scope and object of the certification (including the categories of ICT products, services and processes covered) or how the selected standards or technical specifications – that is, the detailed specification of the cybersecurity requirements, evaluation methods and the intended assurance levels correspond to the needs of the intended users of the said scheme.[17]

As regards the security objectives, article 51 does not only encompass classical computer and information security principles, i.e. the CIA triad[18] and authentication,[19] but broadens the goals of certification schemes to cover more comprehensively cornerstone aspects of cybersecurity such as handling of vulnerabilities,[20] basic digital forensics principles,[21] disaster recovery,[22] security by design and by default,[23] and software & hardware updates.[24] This provision is of utmost importance to address the lack of secure connected products in the Single Market as it lays down essential aspects for the private sector to guarantee (IoT) systems' robustness (Taddeo 2019, 351–52). The attention shall now be turned to the mandatory or voluntary nature of the Cybersecurity Act's measures addressing ICT manufacturers to assess the extent to which the EU cybersecurity certification framework, and notably the cybersecurity objectives outlined in Article 51, can address the lack of secure products in the Single Market.

Recourse to EU cybersecurity certification is, in principle, voluntary. Thus, certifications are in essence voluntary private law instruments, as demonstrated in article 42(3) GDPR[25] in the context of data protection law. Nevertheless, the nature of cybersecurity certification deviates significantly. The European legislator stipulates that Union law, or Member State law – adopted in accordance with Union law – may derogate the general rule.[26] Moreover, in the absence of harmonised Union law, 'Member States are able to adopt national technical regulations providing for mandatory certification under a European cybersecurity certification scheme in accordance with Directive (EU) 2015/1535 of the European Parliament and of the Council'.[27] Thus, the Commission did not want to rule out the possibility to impose specific cybersecurity requirements *via* mandatory certification with the aim of enhancing the level of cybersecurity of the Union, taking into account the existing EU cybersecurity legislation.[28]

Moreover, article 54(3) may offer insight into how the voluntary nature of cybersecurity certifications works in practice with EU cybersecurity legislation. Article 54(3) reads as follows: 'where a specific Union legal act so provides, a certificate or an EU statement of conformity issued under a European cybersecurity certification scheme may be used to demonstrate the presumption of conformity with requirements of that legal act'. A careful examination reveals this provision as an interface between *voluntary* schemes adopted under the Cybersecurity Act and *mandatory* requirements under other Union legal acts. Therefore, the Cybersecurity Act, while reversing the burden of proof, provides a legal basis for the alignment and harmonisation of *mandatory* requirements in EU cybersecurity legislation and *voluntary* certification schemes: even remaining voluntary, the schemes may be used to comply with mandatory requirements of other legal acts.

Although cybersecurity certification initiatives in the IoT field are promoted at national level, such as the Finnish cybersecurity label for IoT (Finnish Transport and Communications Agency 2020), potentially leading to legal fragmentation in the Single Market, the Rolling Plan of the EU Commission did not foresee a cybersecurity certification scheme to directly address the IoT. The Commission focused instead on the need of technical security standards for the IoT, as the lack of interoperability is certainly the thorniest obstacle that still may hinder IoT from its full realisation (Pagallo, Durante, and Monteleone 2017, 74; European Commission 2019, 25), even though ENISA suggested that there is a gap in IoT security standardisation only 'insofar as it is unclear what combination of standards, when applied to a product, service or system, will result in a recognizably secure IoT' (ENISA 2019b, 23). In the 2021 Rolling Plan, the Commission proposed as a priority action to develop a European standard for cybersecurity compliance of products that is aligned with the current information security compliance framework of ISO 27000's family and the GDPR; on the other hand, the standard shall be used to harmonise the requirements set out in the NIS directive (European Commission 2021, 32).

While waiting for a future candidate IoT scheme (ENISA Stakeholder Cybersecurity Certification Group 2021, 10–13), three candidate schemes are under development: the first and more advanced EU Cybersecurity Certification Scheme on Common Criteria (EUCC) (ENISA 2021a, 2021b) – which may serve as a successor to the EU national schemes operating under the SOG-IS MRA, the EU Cybersecurity Certification Scheme on Cloud Services (EUCS) (ENISA 2020a) and the one on 5G.[29] In particular, the EUCC is more of a horizontal scheme:

> it may allow to improve the Internal Market conditions, and to enhance the level of security of ICT products dedicated to security (e.g. firewalls, encryption devices, gateways, electronic signature devices, means of identification such as passports, …) as well as of any ICT product embedding a security functionality (i.e. routers, smartphones, banking cards, medical devices, tachographs for lorries, …). (ENISA 2021a, 11)

As such, IoT manufacturers and developers might consider certifying some ICT products embedded in their IoT solutions. This paradigm has been identified as 'certification by composition': an IoT device may rely on certified components (e.g. firewalls) thanks to the EUCC and on a certified cloud service, thanks to the EUCS (ECSO 2020, 15).

3. Revising EU product legislation: the interplay between the New Legislative Framework and IoT cybersecurity

The cybersecurity of connected products is increasingly considered in the revision process of different legal acts within EU product legislation. This section focuses on four pieces of legislation that show, albeit from different angles, how cybersecurity is progressively linked to the safety regulation of (connected) products; these are: the Radio Equipment

Directive (RED), the Medical Devices Regulation, the Proposal for a Machinery Regulation and the Proposal for a General Product Safety Regulation.

From the adoption of the 'New Approach' in the 80s vis-à-vis product legislation – updated by the so-called 'New Legislative Framework' in 2008,[30] the Union co-legislator has limited product legislation to specifying only the 'essential requirements' (ER) that products have to meet in terms of health and safety (Gorywoda 2009, 163). Rather than adopting overly prescriptive legislation, these requirements are then specified by harmonised technical standards developed by European Standardisation Organisations (ESOs, i.e. ETSI, CEN, CENELEC) on the basis of a mandate of the Commission (Hofmann 2016, 16–17). Most of the legal acts in the area of EU product legislation, and the related harmonised standards specifying the ER thereof, were conceived before the advent of the IoT; in other words, when products were not connected and did not interact with each other or their environment (Fosch-Villaronga and Mahler 2021, 6).

Against this background, the Radio Equipment Directive (RED)[31] is discussed more extensively than the other legal acts. The reason for this is twofold: (i) the recently adopted delegated act to the Directive brings into RED's scope the majority of IoT devices; and (ii) the new legal requirements will oblige manufacturers of wireless devices to include technical features to improve the level of cybersecurity of such devices. Moreover, the legal literature on the topic is rather scarce.

3.1. The radio equipment directive and the delegated regulation 2022/30: strengthening cybersecurity of IoT products

The RED defines 'radio equipment' as an 'electrical or electronic product, which intentionally emits and/or receives radio waves for the purpose of radio communication'.[32] Therefore, 'if IoT devices communicate via radio links, such as Bluetooth or Wi-Fi, they meet the definition of Art. 2 (1) No. 1 RED and are therefore radio equipment within the meaning of RED' (Hessel and Rebmann 2020, 34).

Article 44 RED empowers the Commission to adopt delegated acts specifying which categories or classes of radio equipment were concerned by each of the safety essential requirements of Article 3(3). In this respect, the increasing inclusion of cybersecurity requirements in safety regulation, as exemplified by the RED, shall nonetheless take the distinction between the intertwined concepts of *safety* and *(cyber)security* firm*,* even though the IoT paradigm is blurring the boundary between the two (Vedder 2019, 14–15; Wolf and Serpanos 2020; Chiara 2021).

During the review process, relevant stakeholders highlighted that the cybersecurity standardisation requests of the RED delegated act shall be so open, that they will be reusable in the future horizontal cybersecurity legislation (Wegener 2021), called for by the new cybersecurity strategy (European Commission and the High Representative of the Union for Foreign Affairs and Security Policy 2020, 9), the Council (Council of the European Union 2020, 4–6), the EDPS (European Data Protection Supervisor 2021, 8) and many private actors (BDI, DIN and DKE 2021). Discussions with the ESOs started in September 2019 (Kokx 2021). Eventually, the Commission adopted the delegated regulation on 29 October 2021.[33] The objective of the delegated act is to render the essential requirements set out in Article 3(3)(d), (e) and (f) of the RED applicable to devices capable of communicating over the internet, that is, equipment that constitutes the 'Internet of Things'.

In particular, Article 3(3)(d) mandates that radio equipment does not harm the network or its functioning nor misuse network resources, thereby causing an unacceptable degradation of service; Article 3(3)(e) prescribes that radio equipment incorporates safeguards to ensure that the personal data and privacy of the user and of the subscriber are protected; and Article 3(3)(f) requires that radio equipment supports certain features ensuring protection from fraud.

Whereas Article 3(3)(e) is yet another interface under which we can better appreciate the common approach of EU regulation vis-à-vis cybersecurity and data protection (European Commission and the High Representative of the Union for Foreign Affairs and Security Policy 2020, 4), provided that an artificial distinction between these realms only leads to detrimental effects (Mantelero et al. 2021, 2), Article 3(3)(d) directly concerns 'cybersecurity' as radio equipment will have to incorporate features, that is, cybersecurity measures or controls, to avoid harm, the functioning nor misuse of networks and network resources. As clarified by recital 9 of the Delegated Act, the 'network security' requirement shall be interpreted as broadly to cover main cybersecurity threats,[34] such as DDOS attacks.[35]

Prior to the adoption of the delegated regulation, national competent authorities could not remove IoT products from the market if they fail to comply with the relevant legislation (e.g. the GDPR, the e-Privacy Directive or the incoming ePrivacy Regulation, which would include machine-to-machine communications) (CSES 2020b, 96). Moreover, at the early stages of product's design and engineering, if there was no intention to collect any personal data, manufacturers were not obliged to consider, *inter alia*, data protection by design and by default principles (CSES 2020b, 35). In this scenario, the inherent risk is the potential overlooking of GDPR's security considerations, as the allegedly non-personal data being processed could wrongly justify a lower standard of protection. The broad definition of Article 4(1) GDPR (plus the identifiability test of Recital 26) (Finck and Pallas 2020, 11) and relevant case-law,[36] coupled with the problematic issue of controllership vis-à-vis the 'household exemption' (Finck 2021, 339), implies that EU data protection law would apply to the majority of IoT data processing.

With the adoption of the delegated act, the 'network-preservation' requirement of Article 3(3)(d) would apply to radio equipment that communicates directly or indirectly (i.e. via another equipment) over the internet.[37] Conversely, the privacy & data protection requirement (Article 3(3)(e)) is applicable also to radio equipment designed or intended exclusively for childcare, toys and 'wearables'.[38] Finally, Article 2 of the delegated act derogates from Article 1 by excluding from the scope of all the RED essential requirements medical and in-vitro devices,[39] whilst motor vehicles, electronic road toll systems, equipment to control unmanned aircraft remotely as well as non-airborne specific radio equipment that may be installed on aircrafts are exempt from the requirements regarding the protection of personal data and protection against fraud.[40] Thus, the cybersecurity requirement of Article 3(3)(d) against networks harm and misuse would still be applicable to these legislations.

The adoption of the delegated act would indeed enhance and complement the existing standards of protection under EU cybersecurity and data protection legislation, despite the sectoral scope of the legal act (i.e. wireless devices). All manufacturers of internet-connected and wearable devices must therefore design products that embed baseline cybersecurity and data protection requirements as a pre-condition for market access, even if they claim not to process personal data (CSES 2020a, 5). Cybersecurity and data protection by design would become a condition for market access (CSES 2020a, 37): as a result, national competent authorities – if provided by the Member States with adequate powers and resources vis-à-vis the supervision of consumer products' cybersecurity – will be able to remove non-compliant products from the market.

3.2. The medical devices regulation

Regulation (EU) 2017/745, known as Medical Devices Regulation (MDR), marked the beginning of the incorporation of cybersecurity requirements into EU's safety legal frameworks; for this reason, as mentioned earlier, the Commission exempted such equipment from the scope of the RED.[41] The general safety and performance requirements that medical devices' manufacturers shall achieve are listed in Annex I of the MDR. As regards cybersecurity, devices shall be designed and manufactured to address and minimise 'the risks associated with the possible negative interaction between software and the IT environment within which it operates and interacts'.[42] Moreover, several provisions are dedicated to software. In particular, software should be developed and manufactured 'in accordance with the state of the art taking into account the principles of development life cycle (ENISA 2019a), risk management, including information security, verification'[43] and the specific features of the mobile computing platform in combination with which it is used.[44] The last requirement relevant to cybersecurity addresses 'minimum requirements concerning hardware, IT networks characteristics and IT security measures, including protection against unauthorised access, necessary to run the software as intended'.[45] The MDR addresses cybersecurity requirements to manufacturers, and not other actors involved in the use of a medical devices, such as hospitals and other care providers; (Fosch-Villaronga and Mahler 2021, 7) on the other hand, these actors would be under the scope of the NIS Directive as Operator of Essential Services and thus they are required to manage the cybersecurity risks posed to the network and information systems which they use in their operations (Article 14(1)).

3.3. The Proposal for a General Product Safety Regulation

The Proposal for a General Product Safety Regulation, which would repeal Council Directive 87/357/EEC and Directive 2001/95/EC (General Product Safety Directive, GPSD), is yet another case that enlightens the EU approach towards the introduction of cybersecurity requirements in relevant EU product safety legislation. The analysis of the main legal challenges of the GPSD vis-à-vis safety and cybersecurity risks posed by cyber-physical systems is not new in the legal scholarly literature (Fosch-Villaronga and Mahler 2021, 7–8; Banasinski and Rojszczak 2021, 6–7). On the other hand, the recent proposal for a Regulation has not yet received full attention in terms of its impact in cybersecurity regulation. In this respect, Recital 22 shall be taken into account:

> specific cybersecurity risks affecting the safety of consumers as well as protocols and certifications can be dealt with by sectoral legislation. However, it should be ensured, in case of gaps in the sectoral legislation, that the relevant economic operators and national authorities take into consideration risks linked to new technologies, respectively when designing the

> products and assessing them, in order to ensure that changes introduced in the product do not jeopardise its safety.

Thus, when clarifying the aspects that shall be taken into account for assessing the safety of products, that is, the cases where the presumption of safety laid down in Article 5 does not apply, Article 7 includes 'the appropriate cybersecurity features necessary to protect the product against external influences, including malicious third parties, when such an influence might have an impact on the safety of the product'.[46] To avoid any overlap, it is worth noting how the convergences between the GPSR and RED delegated acts can be exploited. The latter address in part the issue of unsecure connected products in the Single Market. 'However, it will not be possible to cover all possible consumer products via delegated acts, for instance, devices connected by cable. Such gaps might be covered by a revised GPSD in its role of *safety net* [emphasis added]'.[47] In its function of *lex generalis*, it will fully apply to non-harmonised consumer products and to the harmonised consumer products for the aspects that are not covered by harmonised legislation.

3.4. The Proposal for a Regulation on Machinery Products

The Commission is also reviewing the Machinery Directive,[48] albeit currently outside the NLF, to address those cybersecurity risks having an impact on safety, such as preserving machinery against malicious third parties' attacks. The Proposal for a Regulation on Machinery Products,[49] repealing the Directive, would lay down cybersecurity requirements for the design and construction of machinery products[50] while seeking 'to enhance the enforcement of the legal act through the alignment to the NLF' (Anglmayer 2021, 11). It should be noted that the limited scope of the Regulation, which would not apply to household appliances, audio/video equipment, information technology equipment, etc.,[51] would encompass a limited segment of IoT devices, arguably the so-called Industrial IoT or Industry 4.0. In conclusion, the approach of the Commission in trying to deal with the ever-growing number of unsecure IoT devices in the Single Market by amending and strengthening 'type-approval' (Schellekens 2016, 315) legislation, that is, product legislation, shall not be seen as the definitive answer. Product legislation, which primarily targets manufacturers, is focused on the design and manufacturing phases, whereas IoT cybersecurity requires dynamic risk management, that must be ensured throughout the whole life-cycle of the devices (Ducuing 2019, 203). Against this backdrop, the next section sheds light on how new cybersecurity administrative, procedural or organisational aspects introduced by the revision of the NIS Directive may in fact contribute to ensure holistic IoT cybersecurity when coupled with product-related requirements laid down in EU product legislation.

4. Strengthening EU's Cybersecurity: putting the proposal of NIS2 to the test of IoT

This section aims at enlightening to what extent the Proposal for a NIS2 would encompass the complexity and legal challenges in terms of cybersecurity brought about by the IoT. In particular, the analysis aims at testing whether and to what extent the Proposal would ensure a higher standard of protection against unsecure IoT devices by taking into account and addressing the following issues: (i) the enlarged scope of the NIS2, in particular, taking into account 'manufacturing' sector; (ii) the vulnerability disclosure and handling procedures; and, (iii) new cybersecurity requirements for the supply chain.

Without dwelling too extensively on the Directive EU 2016/1148 (NIS Directive) since it does not *specifically* and *directly* cover the IoT, a preliminary remark on the current NIS framework is due to further assess its interplay and possibly regulatory gaps vis-à-vis the IoT cybersecurity, before turning to the Proposal for NIS2. The NIS Directive is the first piece of EU-wide legislation on cybersecurity, providing legal measures to boost the overall level of cybersecurity in the Union. The Directive lays down measures with a view to achieving a high common level of security of network and information systems within the Union. In this respect, the reading of Article 1(7) of the NIS makes it very clear that the Directive must be considered lex generalis vis-à-vis EU sectorial legislation: obligations in terms of networks and information systems security or incident notification imposed by sector-specific Union legal acts on NIS actors must be 'at least equivalent in effect' to the provisions of the Directive to take precedence on the NIS Directive (Ducuing 2021, 2). These actors are classified under two macro-categories, i.e. operators of essential services (OES) and digital service providers (DSP). They operate across vital sectors for EU economy and society, such as energy, transport, water, banking, financial market infrastructures, healthcare. Member states shall identify which entities, either public or private, fall within the definition of OES pursuant to article 5(2) of the Directive.[52] Conversely, the threefold classification of DSP, i.e. online marketplaces, online search engines and cloud computer services,[53] covers every entity falling in one of those categories. Hence, Member states do not have to identify them. A differentiated approach towards OES and DSP has been implemented[54]: 'light-touch' and reactive *ex-post* supervisory activities were accorded to DSP,[55] whereas Member states could impose stricter requirements on OES than those laid down in the Directive (Markopoulou, Papakonstantinou, and De Hert 2019; ENISA 2017, 9). The Directive lays down security and notification requirements for OES at article 14 and for DSP at article 16. The Directive does not give any further indication on the type, appropriateness, and proportionality of technical and organisational measures that OES shall take. These are ultimately assessed by the operators following a risk-based approach, as the European legislator opted for a principles-based model of governance, rather than enforcing prescriptive rules (Cole and Schmitz 2020, 8).[56]

Whilst the NIS Directive did enhance the overall level of cybersecurity in the Union,[57] critical issues have been raised towards the standard of protection it enforced. As the first point of concern, it has been highlighted the risk of legal fragmentation vis-à-vis the possible stricter requirements imposed by national jurisdiction on OES, arguably stemming from the different degrees of cybersecurity preparedness of the Member States (Weber and Studer 2016, 726). The risk of legal fragmentation could also result from the potential overlap of notification requirements under the NIS Directive with other existing breach reporting duties under other EU laws, for example the GDPR (Schmitz-Berndt and Schiffner 2021; Cole and Schmitz 2020; Schmitz-Berndt and Anheier 2021). Furthermore, recital 50 of the NIS Directive, albeit not legally binding (Klimas and Vaiciukaite 2008, 61–94), explicitly excludes from the scope of the Directive hardware manufacturers and software developers, particularly relevant in the domain of IoT, as the European legislator considered the existing rules on product liability to be sufficient.[58] Both the European product liability framework, which dates back to the 1980s, and EU product safety legislation, as shown in the previous section, are in the midst of a thorough overhaul to assess the impact of so-called digital emerging technologies, especially in terms of (cyber)security.[59] Given that these actors supply solutions that form the backbone of the network and information systems of DSPs and OESs and they are likely to maintain a crucial role during the lifecycle of their products and services (e.g. in terms of patching), it is reasonable asking whether and to what extent it is fair to hold responsible – and ultimately liable – solely the OES and the DSP for cybersecurity incidents that are hardly within their control. Thus, the evaluation of the functioning of the NIS Directive highlighted as a major area of concern the too limited scope of the Directive.[60]

The Proposal acknowledges that the increased digitisation in the recent years and the higher rate of interconnectedness are crucial factors that contributed to the gradual inadequacy of the too limited scope of the NIS Directive, which no longer reflects all digitised sectors providing key services to the Union.[61] Arguably, it is safe to say that the IoT, implicitly recalled by the legislator with the buzzword's 'interconnectedness' and 'digitisation', is in this regard one of the game-changers that led to this paradigm shift. As regards the determination of entities falling within the scope of NIS2, it is suggested to abandon the distinction between OES and DSP. Rather, the new Directive will apply to public and private 'essential' and 'important' entities, with the same obligations, referred to in the lists of economic sectors of Annex I and II to the Proposal respectively.[62]

To overcome the wide divergences among Member States, Article 2(1) lays down as a criterion to determine which entity falls into the scope of the Directive a 'size-cap rule', whereby all small and micro enterprises would fall outside the scope of protection. Nevertheless, recital 9 claims for an exception: 'small or micro entities fulfilling certain criteria that indicate a key role for the economies or societies of Member States or for particular sectors or types of services, should also be covered by this Directive'.[63] Accordingly, article 2(2) states that, regardless of their size, this Directive also applies to essential and important entities if the actor under scrutiny fulfils certain requirements.[64] On the one hand, the rationale of such broad scope is clearly to provide comprehensive coverage of the sectors of vital importance for key societal and economic activities[65]; on the other, the absence of granular and scalable requirements based on actual risk (e.g. business-to-business versus business-to-consumer models) may become 'a blanket legislation covering most ICT services without any real distinctions' (DIGITALEUROPE 2021a, 4; BDI 2021b, 7).

Importantly, Annex II lists as 'important entities' the manufacturing sector. All the six sub-sectors included (medical, computer, electronic, electrical, machinery, motor vehicles and transport equipment) are highly relevant for the IoT market: these are further specified by the NACE Rev. 2 classification of economic activities. For example, the manufacturing of computers and electronic products includes *inter alia* consumer electronics, electronics components and communication equipment.[66] It should be excluded that the rationale of including such broad manufacturing categories is to *directly* tackle the problem of (IoT) unsecure products and services, as already product sectoral legislation – such as the RED delegated act – mandates cybersecurity technical requirements (DIGITALEUROPE 2021a, 6). Rather, connected devices forming part of the network and information systems of 'essential' and 'important' entities would still be covered by the scope *rationae personae* of the NIS 2 vis-à-vis network and information systems' risk management and notification obligations. In light of the principle-based character of the NIS2, the Proposal introduces procedural, or 'organisational' (DIGITALEUROPE 2021b, 9), requirements that would complement the objectives of protection of EU product safety legislation vis-à-vis (IoT) cybersecurity. In particular, this would be the case vis-à-vis: (i) the disclosure and handling procedures for vulnerabilities; (ii) cybersecurity requirements in terms of secure supply chain relationships.

Article 6 of the Proposal establishes conditions and a procedural framework for coordinated vulnerability disclosure. This framework hinges on the intermediary role of CSIRTs and ENISA: the former shall facilitate the interaction between the reporting entity and the manufacturer,[67] whilst the latter shall develop and maintain a European vulnerability database leveraging the global Common Vulnerabilities and Exposures (CVE) accessible to all interested parties.[68] Importantly, the original text proposed by the Commission has been amended by the Parliament so to specify that only those vulnerabilities for which a patch is available shall be listed in the vulnerability database.[69] Otherwise, a paradoxical situation could have arisen where a vulnerability was published without any mitigation measures, thus facilitating the work of attackers. Against this background, the legislative text acknowledges that 'entities that develop such systems should therefore establish appropriate procedures to handle vulnerabilities when they are discovered[.] The manufacturer or provider of ICT products or services should also put in place the necessary procedures to receive vulnerability information from third parties'.[70] Nevertheless, the Proposal does not foresee an 'obligation to patch' within a specific timeframe for manufacturers (European Commission 2013, 9), thus addressing at the core the problem of unsecure systems. While it is welcomed by industry on the grounds that companies, when developing patches, 'should not encounter additional outside pressure which could lead to a deterioration of the quality of the work',[71] the freedom and trust entitled to manufacturers may come at a cost for consumers in terms of security.

Another important aspect that may intersect with considerations on 'products cybersecurity' is the emphasis put on the security of supply chain relationships. The majority of IoT devices is comprised from a multitude of components from different hardware and software vendors, part of which could even be accounted for by small companies, including start-ups (European Commission 2020).[72] This results in a global expansion of the attack surface (AIOTI 2021, 3). Recent discussions, both in Europe and in the US, find a consensus that supply chain security is crucial in IoT (Council of the European Union 2020, 3): ENISA and the US National Institute of Standards and Technology (NIST) acknowledge that securing supply chain represents both a challenge and an opportunity. On the one hand, it lays down the foundation for devices' security, and on the other hand, it raises concerns since organisations are hardly aware of the security measures adopted by supply chain partners (ENISA 2020b, 5; NIST 2021, 13). In this respect, ENISA mapped out the entire lifespan of the IoT supply chain – hardware, software and services – by offering security measures for each step (ENISA 2020b, 9). Unlike NIS 1, Article 18(2) specifies a minimum list of cybersecurity measures[73] that entities have to adopt vis-à-vis the management of risks to their network and information systems (Article 18(1)) (Sievers 2021). In particular, letter (d) addresses supply chain security including security-related aspects concerning the relationships between each entity and its suppliers. Importantly, the Proposal specifies at Article 18(3) that NIS2 entities, when implementing measures referred to letter (d), 'shall take into account the vulnerabilities specific to each supplier and service provider and the overall *quality of products* and cybersecurity practices of their suppliers and service providers [emphasis added]'. Whereas the Union legislature has yet to clarify how NIS2 entities shall ensure that suppliers comply with the legal requirements (BDI 2021b, 15; DIGITALEUROPE 2021a, 7), this provision would *indirectly* address products security because, by requiring to consider systems' cybersecurity of suppliers, manufacturers will have strong incentives to enhance the security controls in their products.

5. Conclusion

The technical multi-layered complexity of the IoT ecosystem makes it hard to establish safeguards and ensure adequate levels of security and safety. The lesson learned in recent years by European Union countries is that there is no silver bullet since the risk is a very context-dependent variable. In any given sector, the risk profile is not the same for all IoT product categories; for a given IoT product category, the risk profile is not the same across sectors.

The majority of EU Member States had opted for voluntary approaches to IoT products security – afraid that regulation could stifle either innovation or competition. Nonetheless, several factors have pushed EU Institutions to (re)act: on the one hand, the increasing expansion of the attack surface, the growing scale and complexity of the cyberthreat (ENISA 2020c), and on the other hand, market asymmetries and regulatory failures in the ICT/IoT sector (Kopp, Kaffenberger, and Wilson 2017).

The study commissioned by the Commission on the need for cybersecurity requirements for ICT products highlighted three main regulatory failures vis-à-vis the current state of connected products security: (i) the absence of mandatory requirements (e.g. no clear obligations for the manufacturer); (ii) the lack of common legal basis that sets cybersecurity requirements for ICT products; (iii) the absence of rules for post-market surveillance, with regards to cybersecurity (Wavestone 2021, 69). As stressed in the Introduction, this contribution has focused on the first aspect i.e. IoT manufacturers' obligations in relation to cybersecurity requirements.

Overall, it appears that the European cybersecurity legal frameworks aim to tackle cybersecurity incidents and vulnerabilities while enhancing the security of key economic sectors within the Union. Nevertheless, they do not target IoT products specifically, as described in the legal analysis.

The first legal act under scrutiny was the Cybersecurity Act. Considering the EU cybersecurity certification framework as *purely* voluntary is rather inaccurate. Rather, the legislator expressly left open the possibility of imposing specific cybersecurity requirements and making the certification thereof mandatory. Moreover, Member State law or other Union legal acts can provide for legally binding schemes, as confirmed in Article 21 of the Proposal for NIS2. Notwithstanding the negative externalities arising from the high costs and low incentives (Wavestone 2021, 72), the ENISA conference on cybersecurity certification of 2–3 December 2021,[74] stressed the key competitive advantage that comes along with certification, as most of the customers and a significantly large part of the vendors of the supply chain look for certified products, services and processes, even if this would cost them more (Blythe, Johnson, and Manning 2020). In other words, market dynamics increasingly tend to make these private law instruments *de facto*, but not *de jure*, 'mandatory'.

Then, several legislative texts under the New Legislative Framework were analysed to highlight the increasing inclusion of mandatory cybersecurity requirements in EU product safety legislation. Hence, the Commission deemed it reasonable to first tackle the issue of unsecure connected products from a sectoral viewpoint rather than embarking on a long legislative process in view of the introduction of a horizontal piece of legislation on cybersecurity.[75] The RED, and in particular the Delegated Act activating Article 3(3)(d), (e), and (f) casts light on the action of the Commission addressing the abovementioned regulatory failures: national market surveillance authorities will ensure that all manufacturers of wireless devices comply with the new obligations to increase the level of cybersecurity (and privacy & data protection too) of products placed on the EU market.

Finally, the proposal for a NIS2 considerably strengthens the level of protection offered by the NIS Directive. This article demonstrated that the IoT ecosystem (i.e. manufacturers and developers of final ICTs products and services along the whole supply chain) would benefit from the policy changes introduced by the NIS2, as it would strengthen and complements the EU cybersecurity regulatory landscape. In this respect, the article has shed light on three decisive actions that regard: (i) an enlarged scope of the new Directive, including in particular (IoT) manufacturing; (ii) a procedure for the disclosure and handling of vulnerabilities; and, (iii) stronger and detailed cybersecurity risk management requirements for covered entities with a major emphasis on supply chain security.

This article further demonstrated that whilst a sectoral approach vis-à-vis the issue of connected products security may prove to be effective in the short term, only horizontal legislation will efficiently address the problem at the core (Wavestone 2021, 256–57). Thus, it is necessary to harmonise a highly fragmented regulatory landscape, as seen in section 3, and avoid overlapping requirements stemming from different pieces of legislation.

Horizontal legislation has been proposed and endorsed by the EU Council, the Commission and many industrial associations (Council of the European Union 2020, 4; European Commission and the High Representative of the Union for Foreign Affairs and Security Policy 2020, 9; BDI 2021b; Orgalim 2020, 4–6), and it should be developed by following the principles of the New Legislative Framework. This policy option, to appropriately tackle existing regulatory failures, should pivot on three building blocks: mandatory cybersecurity essential requirements for all connected products; reference to European harmonised technical standards and conformity assessment; and market surveillance. On the seemingly problematic interplay between vertical and horizontal legislation, to avoid duplicative or conflicting obligations, cybersecurity essential requirements introduced by sectoral EU product legislation should be repealed once horizontal legislation enters into force.

In this regard, it is worth noting that the Council's call for coordination and cooperation with all relevant public and private stakeholders, such as the Commission, the ENISA, the Telecommunication Conformity Assessment and Market Surveillance Committee, the European Cybersecurity Certification Group (ECCG) and, on the other hand, small and medium enterprises (SMEs) is essential for the European cybersecurity regulatory landscape (Council of the European Union 2020, 5–7). This co-regulatory and inclusive approach is likely to be more effective than a top-down model of governance (Pagallo, Casanovas, and Madelin 2019) which would exclude crucial actors from the decision-making process, since cybersecurity is a shared responsibility (Taddeo 2019, 351; Brighi and Chiara 2021).

Notes

1. The pervasive and multi-device nature of IoT is increasingly leading to review the original acronym, as some prefers the term Internet of Everything (IoE); CISCO, 'How does Cisco define the Internet of Everything, and how is it different from the "Internet of Things"?' (2013), available at: https://www.cisco.com/c/dam/en_us/about/business-insights/docs/ioe-value-at-stake-public-sector-analysis-faq.pdf.
2. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).
3. Regulation (EU) 2019/881, Article 2(1).
4. Regulation (EU) 2019/881, Article 68(4).
5. Article 4 of Regulation (EU) 2019/881 outlines the main objectives of the Agency, such as assisting Union institutions, bodies, offices, agencies as well as Member states in implementing EU policies on cybersecurity, supporting capacity-building and preparedness across the Union, promoting cooperation, including information-sharing and coordination at Union level, contributing to increasing cybersecurity capabilities and promoting the use of EU cybersecurity certification.
6. Article 5 of Regulation (EU) 2019/881 mainly refers to 3 strands of actions: *assisting* in the development, review, implementation of Union cybersecurity policy and law; *contributing* to the work of the Cooperation group; *supporting* the development and implementation of cybersecurity policy in Union legislation as well as the regular review of Union policy through an annual report on the state of the implementation of the respective legal framework.
7. Regulation (EU) 2019/881, recital 19.
8. Regulation (EU) 2019/881, Article 3(1).
9. Regulation (EU) 2019/881, recital 69.
10. Regulation (EU) 2019/881, Article 2(12).
11. Regulation (EU) 2019/881, Article 2(13).
12. Regulation (EU) 2019/881, recital 2.
13. Regulation (EU) 2019/881, recital 65.
14. Regulation (EU) 2019/881, Article 58.
15. Regulation (EU) 2019/881, Article 60.
16. Regulation (EU) 2019/881, Article 53.
17. Regulation (EU) 2019/881, Article 54(1); recital 84.
18. Regulation (EU) 2019/881, Article 51, letters (a) and (b).
19. Regulation (EU) 2019/881, Article 51, letter (c).
20. Regulation (EU) 2019/881, Article 51, letters (d) and (g).
21. Regulation (EU) 2019/881, Article 51, letters (e) and (f).
22. Regulation (EU) 2019/881, Article 51, letter (h).
23. Regulation (EU) 2019/881, Article 51, letter (i).
24. Regulation (EU) 2019/881, Article 51, letter (j).
25. Regulation (EU) 2016/679, Article 42(3): 'the certification shall be voluntary and available via a process that is transparent'.
26. Regulation (EU) 2019/881, Article 56(2); recital 91.
27. Regulation (EU) 2019/881, recital 91.
28. Regulation (EU) 2019/881, recital 92.
29. See <https://www.enisa.europa.eu/topics/standards/adhoc_wg_calls/ad-hoc-working-group-on-5g-cybersecurity-certification> accessed 18 December 2021.
30. The New Legislative Framework aims at improving the internal market for goods and strengthens the conditions for placing a wide range of products on the market (CE marking), via a package of measures which improves market surveillance and boosts the quality of conformity assessments. These measures are: Regulation EU 765/2008; Decision

768/2008; Regulation EU 2019/1020. European Commission, 'The "Blue Guide" on the Implementation of EU Products Rules 2016 (2016/C 272/01)' [2016] Official Journal of the European Union, 9–10.

31. Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC Text with EEA relevance.
32. Directive 2014/53/EU, Article 2(1)(1).
33. Commission Delegated Regulation (EU) 2022/30 of 29.10.2021 supplementing Directive 2014/53/EU of the European Parliament and of the Council with regard to the application of the essential requirements referred to in Article 3(3), points (d), (e) and (f), of that Directive.
34. RED delegated act, recital 9: 'an attacker may maliciously flood the internet network to prevent legitimate network traffic, disrupt the connections between two radio products, thus preventing access to a service, prevent a particular person from accessing a service'.
35. *Contra* see Cezary Banasinski and Marcin Rojszczak, 'Cybersecurity of Consumer Products against the Background of the EU Model of Cyberspace Protection' (2021) 00 Journal of Cybersecurity 1, 7.
36. CJEU, Case C-582/14, Patrick Breyer v Bundesrepublik Deutschland (2016); CJEU, Case C-434/16 Peter Nowak v Data Protection Commissioner (2017).
37. RED delegated act, Article 1(1).
38. RED delegated act, Article 1(2).
39. RED delegated act, Article 2(1).
40. RED delegated act, Article 2(2).
41. RED delegated act, recital 15.
42. MDR, Annex I, 14.2(d).
43. MDR, Annex I, 17.2
44. MDR, Annex I, 17.3.
45. MDR, Annex I, 17.4.
46. Proposal for a Regulation on General Product Safety, Article 7(h).
47. European Commission, 'Commission Staff Working Document Impact Assessment accompanying the document Proposal for a Regulation of the European Parliament and of the Council on general product safety, amending Regulation (EU) No 1025/2012 of the European Parliament and of the Council, and repealing Council Directive 87/357/EEC and Directive 2001/95/EC of the European Parliament and of the Council' SWD(2021) 169 final, 10.
48. Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on machinery.
49. European Commission, 'Proposal for a Regulation of the European Parliament and of the Council on machinery products' COM(2021) 202 final.
50. Essential Health and Safety Requirements (EHSR) in Annex III will be modified to address cybersecurity issue with an impact on safety: (i) EHSR 1.1.9: security by design of machinery products; (ii) EHSR 1.2.1: security by design of control systems.
51. Proposal for a Regulation on Machinery Products, article 2(2)(m).
52. NIS Directive, art. 5(2): the entity provides a service that is essential for the maintenance of critical societal and/or economic activities; the provision of the service depends on network and information systems; and, incidents would have significant disruptive effects on the provision of the service.
53. NIS Directive, Annex III.
54. This has been justified by the direct link with physical infrastructure of the former compared to the cross-border nature of the latter (recital 57).
55. NIS Directive, recital 60; Article 17(1).
56. NIS Directive, art. 14; Mark D Cole and Sandra Schmitz, 'The Interplay Between the NIS Directive and the GDPR in a Cybersecurity Threat Landscape' (2020) SSRN Electronic Journal, 8: '[w]hile the national transposition of the NIS Directive repeat the general wording of the Directive, complementary guidance or regulations amending national law define the indefinite legal concepts further'.

57. European Commission, ‘Proposal for a Directive of the European Parliament and the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148’ COM(2020) 823, 2.
58. NIS Directive, recital 50.
59. European Commission – Expert Group on Liability and New Technologies, ‘Liability for Artificial Intelligence and Other Emerging Digital Technologies’ (2019): the report, released at the end of November 2019, is the final deliverable of the Expert Group on liability and new technologies appointed by the European Commission in March 2018.
60. Proposal for NIS2, 6.
61. ibid, 6.
62. ibid, Article 2(1).
63. ibid, recital 9.
64. ibid, Article 2(2). Notably, article 5(2)(h) would mandate Member States to adopt, as part of the national cybersecurity strategy, a ‘policy addressing specific needs of SMEs, in particular those excluded from the scope of this Directive, in relation to guidance and support in improving their resilience to cybersecurity threats’.
65. Ibid, recital 7.
66. NACE Rev. 2 – Statistical classification of economic activities in the European Community, division 26, 69.
67. Proposal for NIS2, Article 6(1).
68. Draft European Parliament legislative resolution on the 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)0823 – C9-0422/2020 – 2020/0359(COD)), amendment 127.
69. id.
70. Proposal for NIS2, recital 28.
71. BDI, Position on ITRE-Amendments to NIS 2-Directive German industry’s position on the ITRE Committee’s amendments to the Commission proposal for a Directive on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148, 6.
72. See <https://www.startus-insights.com/innovators-guide/5-top-internet-of-things-startups-impacting-logistics-supply-chain/> accessed 21 October 2021.
73. The list includes risk analysis and information security policies, incident handling, use of cryptography and encryption, business continuity, testing and auditing procedures to assess the effectiveness of the cybersecurity measures.
74. See <https://www.enisa.europa.eu/news/enisa-news/going-full-throttle-on-cybersecurity-certification-and-market> accessed 3 December 2021.
75. RED delegated act, 5.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Funding

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie ITN EJD grant agreement No 814177.

References

AIOTI. 2021. “AIOTI Feedback to the Public Consultation on the Revised Draft NIS Directive (NIS2)”.

Anglmayer, I. 2021. *Briefing Implementation Appraisal – Machinery Directive Revision of Directive 2006/42/EC (2021)*, EPRS, European Parliament, 11.

Banasinski, C., and M. Rojszczak. 2021. "Cybersecurity of Consumer Products against the Background of the EU Model of Cyberspace Protection." *Journal of Cybersecurity* 7 (1): 1–15.

BDI. 2021b. "Position Paper on NIS 2-Directive".

BDI. Position on ITRE-Amendments to NIS 2-Directive German industry's position on the ITRE Committee's amendments to the Commission proposal for a Directive on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148.

BDI, DIN and DKE. 2021. "EU-wide Cybersecurity Requirements – Introduction of Horizontal Cybersecurity Requirements Based on the New Legislative Framework and Bridge to the EU Cybersecurity Act" Position Paper.

Blythe, J. M., S. D. Johnson, and M. Manning. 2020. "What Is Security Worth to Consumers? Investigating Willingness to Pay for Secure Internet of Things Devices." *Crime Science* 9: 1.

Bormann, C., M. Ersue, and A. Keranen. 2014. "Terminology for Constrained-Node Networks". *Internet Engineering Task Force* (IETF – 7228).

Brighi, R., and P. G. Chiara. 2021. "La Cybersecurity Come Bene Pubblico: Alcune Riflessioni Normative a Partire Dai Recenti Sviluppi Nel Diritto Dell'Unione Europea." *Federalismi.it*, 21, 18.

Cheruvu, S., A. Kumar, N. Smith, and D. Wheeler. 2020. *Demystifying Internet of Things Security: Successful IoT Device/Edge and Platform Security Deployment*. Berkeley, CA: Apress Open.

Chiara, P. G. 2021. "The Balance Between Security, Privacy and Data Protection in IoT Data Sharing: A Critique to Traditional "Security&Privacy" Surveys." *European Data Protection Law Review* 7: 18–30.

Cole, M. D., and S. Schmitz. 2020. "The Interplay Between the NIS Directive and the GDPR in a Cybersecurity Threat Landscape." University of Luxembourg Law Working Paper No. 2019-017.

Council of the European Union. 2020. "Council Conclusions on the Cybersecurity of Connected Devices" 13629/20.

CSES. 2020a. "Executive Summary – Impact Assessment on Increased Protection of Internet-Connected Radio Equipment and Wearable Radio Equipment".

CSES. 2020b. "Final Report – Impact Assessment on Increased Protection of Internet-Connected Radio Equipment and Wearable Radio Equipment".

Denardis, L. 2020. *The Internet in Everything – Freedom and Security in a World with No Off Switch*. New Haven: Yale University Press.

DIGITALEUROPE. 2021a. "DIGITALEUROPE Position on the NIS2 Directive".

DIGITALEUROPE. 2021b. "Setting the Standard: How to Secure the Internet of Things".

Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on machinery.

Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC Text with EEA relevance.

Ducuing, C. 2019. "Towards an Obligation to Secure Connected and Automated Vehicles "by Design"?" In *Security and Law: Legal and Ethical Aspects of Public Security, Cyber Security and Critical Infrastructure Security*, edited by A. Vedder, J. Schroers, C. Ducuing, and P. Valcke, 183–214. Cambridge: Intersentia.

Ducuing, C. 2021. "Understanding the Rule of Prevalence in the NIS Directive: C-ITS as a Case Study." *Computer Law and Security Review* 40: 105514.

Durante, M. 2021. *Computational Power: The Impact of ICT on Law, Society and Knowledge*. Abingdon: Routledge.

ECSO. 2020. "European Cyber Security Certification – Challenges Ahead for the Roll-Out of the Cybersecurity".

ENISA. 2017. *Incident Notification for DSPs in the Context of the NIS Directive – A Comprehensive Guideline on How to Implement Incident Notification for Digital Service Providers, in the Context of the NIS Directive*.

ENISA. 2019a. "Good Practices for Security of IoT Secure Software Development Lifecycle".

ENISA. 2019b. "IoT Security Standards Gap Analysis: Mapping of Existing Standards against Requirements on Security and Privacy in the Area of IoT".

ENISA. 2020a. "EUCS – CLOUD SERVICES SCHEME: EUCS, a Candidate Cybersecurity Certification Scheme for Cloud Services".

ENISA. 2020b. "Guidelines for Securing the Internet of Things – Secure Supply Chain for IoT".

ENISA. 2020c. "The Year in Review: ENISA Threat Landscape".

ENISA. 2021a. "Cybersecurity Certification: Candidate EUCC Scheme V1.1.1".

ENISA. 2021b. "Public Consultation on the Draft Candidate EUCC Scheme".

ENISA Stakeholder Cybersecurity Certification Group. 2021. "Consultation Report on Draft URWP".

European Commission. 2013. "Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace JOIN(2013) 1 Final".

European Commission. 2017. "Joint Communication to the European Parliament and the Council Resilience, Deterrence and Defence: Building Strong Cybersecurity for the EU".

European Commission. 2019. "Rolling Plan for ICT Standardisation 2019".

European Commission. 2020. "An SME Strategy for a Sustainable and Digital Europe" COM(2020) 103 final.

European Commission. 2021. "Rolling Plan for ICT Standardisation 2021".

European Commission and the High Representative of the Union for Foreign Affairs and Security Policy. 2020. "Joint Communication to the European Parliament and the Council: The EU's Cybersecurity Strategy for the Digital Decade".

European Data Protection Supervisor. 2021. "Opinion 5/2021 on the Cybersecurity Strategy and the NIS 2.0 Directive".

European Union Agency for Fundamental Rights. 2018. *Manuale sul diritto europeo in materia di protezione dei dati*. Lussemburgo: EU Publishing Office.

Finck, M. 2021. "Cobwebs of Control: The Two Imaginations of the Data Controller in EU Law." *International Data Privacy Law* 11: 333–347.

Finck, M., and F. Pallas. 2020. "They Who Must Not Be Identified—Distinguishing Personal from Nonpersonal Data Under the GDPR." *International Data Privacy Law* 10: 11–36.

Finnish Transport and Communications Agency. 2020. "Finnish Cybersecurity Label." https://tietoturvamerkki.fi/files/cybersecurity_label_presentation-280920.pdf.

Fosch-Villaronga, E., and T. Mahler. 2021. "Cybersecurity, Safety and Robots: Strengthening the Link Between Cybersecurity and Safety in the Context of Care Robots." *Computer Law & Security Review* 41: 105528.

Fuster, G. G., and L. Jasmontaite. 2020. "Cybersecurity Regulation in the European Union: The Digital, the Critical and Fundamental Rights." In *The Ethics of Cybersecurity*. Vol. 21, edited by M. Christen, B. Gordijn, and M. Loi, 97–115. Cham: Springer.

Giovanni, C., and F. Silva. 2018. "Cybersecurity for Connected Products" (2018) ANEC and BEUC position paper, ANEC-DIGITAL-2018-G-001final – BEUC-X-2018-017 07/03/2018.

Gorywoda, L. 2009. "The New European Legislative Framework for the Marketing of Goods." *Columbia Journal of European Law* 16: 161.

Hessel, S., and A. Rebmann. 2020. "Regulation of Internet-of-Things Cybersecurity in Europe and Germany as Exemplified by Devices for Children." *International Cybersecurity Law Review* 1: 27–37.

Hofmann, H. C. H. 2016. "European Regulatory Union? The Role of Agencies and Standards." In *Research Handbook on the EU's Internal Market*, edited by P. Koutrakos, and J. Snell, 460–478. Cheltenham: Elgar Publishing.

Kamara, I. 2021. "Misaligned Union Laws? A Comparative Analysis of Certification in the Cybersecurity Act and the General Data Protection Regulation." In *Data Protection and Privacy: Data Protection and Artificial Intelligence*, edited by D. Hallinan, R. Leenes, and P. De Hert, 83–110. London: Hart Publishing.

Klimas, T., and J. Vaiciukaite. 2008. "The Law of Recitals in European Community Legislation." *ILSA Journal of International & Comparative Law* 15: 1.

Kokx, B. 2021. "European Standardization Organisations" ENISA Cybersecurity Standardization Conference, Panel 2: Radio Equipment Directive – Setting Up the Scene and Future Wo Cybersecurity and Radio Equipment Directive – Implementing Measures.

Kopp, E., L. Kaffenberger, and C. Wilson. 2017. "Cyber Risk, Market Failures, and Financial Stability." International Monetary Fund Working Paper.

Mantelero, A., G. Vaciago, M. S. Esposito, and N. Monte. 2021. "The Common EU Approach to Personal Data and Cybersecurity Regulation." *International Journal of Law and Information Technology* 28 (4): 297–328.

Markopoulou, D., V. Papakonstantinou, and P. De Hert. 2019. "The new EU Cybersecurity Framework: The NIS Directive, ENISA's Role and the General Data Protection Regulation." *Computer Law & Security Review* 35 (6): 105336.

NIST. 2021. "Workshop Summary Report for "Building the Federal Profile for IoT Device Cybersecurity" Virtual Workshop – NISTIR 8322".

Orgalim. 2020. "Proposal for a Horizontal Legislation on Cybersecurity for Networkable Products within the New Legislative Framework." Position Paper.

Pagallo, U., P. Casanovas, and R. Madelin. 2019. "The Middle-out Approach: Assessing Models of Legal Governance in Data Protection, Artificial Intelligence, and the Web of Data." *Theory and Practice of Legislation* 7 (1): 1–25.

Pagallo, U., M. Durante, and S. Monteleone. 2017. "What Is New with the Internet of Things in Privacy and Data Protection? Four Legal Challenges on Sharing and Control in IoT." In *Data Protection and Privacy: (in) Visibilities and Infrastructures*, edited by Ronald Leenes, Rosamunde van Brakel, Serge Gutwirth, and Paul De Hert, 59–78. Cham: Springer.

Rayes, A., and S. Salam. 2019. *Internet of Things: From Hype to Reality*. Cham: Springer.

Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on Information and Communications Technology Cybersecurity Certification and Repealing Regulation (EU) No 526/2013 (Cybersecurity Act).

Schellekens, M. 2016. "Car Hacking: Navigating the Regulatory Landscape." *Computer Law and Security Review* 32: 307–315.

Schmitz-Berndt, S., and F. Anheier. 2021. "Synergies in Cybersecurity Incident Reporting – The NIS Cooperation Group Publication 04/20 in Context." *European Data Protection Law Review* 7: 101–107.

Schmitz-Berndt, S., and S. Schiffner. 2021. "Don't Tell Them Now (Or at All) – Responsible Disclosure of Security Incidents Under NIS Directive and GDPR." *International Review of Law, Computers & Technology* 35: 101–115.

Sievers, T. 2021. "Proposal for a NIS Directive 2.0: Companies Covered by the Extended Scope of Application and Their Obligations." *International Cybersecurity Law Review* 2: 223–231.

Spagnuelo, D., A. Ferreira, and G. Lenzini. 2019. "Accomplishing Transparency within the General Data Protection Regulation." In *Proceedings of the 5th International Conference on Information Systems Security and Privacy* (ICISSP 2019).

Stahl, K., and R. Strausz. 2017. "Certification and Market Transparency." *Review of Economic Studies* 84: 1842.

Stapko, T. 2008. *Practical Embedded Security: Building Secure Resource-Constrained Systems* . Burlington, MA: Newnes.

Taddeo, M. 2019. "Is Cybersecurity a Public Good?" *Minds and Machines* 29: 349–354.

Vedder, A. 2019. "Safety, Security and Ethics." In *Security and Law: Legal and Ethical Aspects of Public Security, Cyber Security and Critical Infrastructure Security*, edited by A. Vedder, J. Schroers, C. Ducuing, and P. Valcke, 11–26. Cambridge: Intersentia.

Wavestone – CEPS – CARSA – ICF. 2021. "Study on the Need of Cybersecurity Requirements for ICT Products - No. 2020-0715: Final Study Report".

Weber, R. H., and E. Studer. 2016. "Cybersecurity in the Internet of Things: Legal Aspects." *Computer Law & Security Review* 32: 715–728.

Wegener, D. 2021. "Proposal for a realistic way to implement a 'Cybersecurity regulation in Europe'" ENISA Cybersecurity Standardization Conference, panel 1: Cybersecurity and Radio Equipment Directive – setting up the scene and future work.

Wolf, M., and D. Serpanos. 2020. *Safe and Secure Cyber-Physical Systems and Internet-of-Things Systems*. Cham: Springer.