Check for updates

Article

Wilfried Martens Centre for European Studies

European View
2022, Vol. 21(2) 186–195
© The Author(s) 2022
DOI: 10.1177/17816858221136106
journals.sagepub.com/home/euv
SAGE

In a hyperconnected world, is the EU cybersecurity framework connected?

Iva Tasheva and Ilana Kunkel

Abstract

This article sheds light on the fast-evolving and ever more complex EU cybersecurity policy. It shows that horizontal and sector-specific regulation are being developed simultaneously. It identifies the gaps and investigates to what extent the new Cyber Resilience Act and other policy instruments might address them. It first reviews the stock of existing EU legislation before examining the relevant industry standards for cybersecurity and the Internet of Things. It also reviews stakeholders' expectations for the Cyber Resilience Act and identifies the need for horizontal legislation, setting flexible but binding rules. We argue for horizontal standards (process-based) that are complemented by sector-specific (vertical) standards. Finally, we propose a governance and enforcement model to make the cybersecurity framework better coordinated and more adequate for tackling the ever-evolving cybersecurity threat landscape.

Keywords

Cybersecurity, EU policy, Cyber resilience, IoT, EU Cyber Resilience Act, EU legislation, EU NIS Directive, EU Medical Devices Regulation, New legislative framework

Introduction

In September 2022, one year after its announcement by the European Commission President Ursula von der Leyen, the proposal for a Cyber Resilience Act to set common EU cybersecurity standards has been published (Von der Leyen 2021, European Commission 2022b). Cyber resilience is highlighted as one of the top priorities for the Union during the 2019–24 Commission term (European Commission 2020b). The aim of resilience is to prevent cyber-attacks and mitigate their impact by ensuring that digital

Corresponding author:
Iva Tasheva, Cyen, Avenue Paul Hymans 121, Brussels, 1200, Belgium.
Email: iva.tasheva@cyen.eu

products and software still function in the intended manner even if a security incident occurs.

Since 2020, the EU has produced numerous legislative initiatives on cybersecurity. The EU directive on the security of network and information systems (the NIS Directive (EU 2016/1148)), which was adopted in 2016, has been reviewed to expand its scope and reach. Specific cybersecurity requirements have also been introduced or are in the process of being introducedfor artificial intelligence (AI) systems (2021 AI Act proposal (COM(2021) 206 final)), medical devices (the Medical Device Regulation, MDR) and the Internet of Things (IoT, Delegated Act under the Radio Equipment Directive). The Machinery and the General Product Safety Directives are also under review to take into consideration cybersecurity factors. In addition, the new Cyber Resilience Act presented on 15 September 2022 is a horizontal piece of legislation, complementing the EU NIS Directive to cover a wide range of digital products (European Commission 2022b). Most of these new obligations will become applicable by approximately 2024.

The IoT is a focal point in emerging cybersecurity challenges. By 2025, there will be 30.9 billion IoT devices globally and 4.3 billion in Europe (Statista 2021). Today, the number of IoT devices already outnumbers the number of people on the globe (European Commission 2020b). If not secure, these devices could all be used in a large-scale attack, such as a massive botnet attack on critical infrastructure (an attack using hijacked connected devices such as IoT devices or laptops to launch an orchestrated offence on a final target). In addition, the nature of IoT applications often involves sensitive data (e.g. medical IoT devices) or/and data being shared between devices without human intervention (e.g. automatic garage doors and connected cars). The rise of the IoT and its vulnerabilities, coupled with a lack of legislation that tackles the complex challenges of connected devices, make the IoT a crucial use case for future legislation.

This article looks at the existing EU cybersecurity framework to identify gaps in the regulatory landscape, focusing on the IoT use case. It also considers the approach of the member states, industry and existing IoT cybersecurity standards, providing policy recommendations for the European Commission that will strengthen the EU cybersecurity legislative landscape and that should be considered in the upcoming legislative process. The authors argue that the EU cybersecurity legislative framework is quickly developing and becoming ever more complex. Yet there are significant gaps and areas where further action is needed to make it effective. Before arriving at this conclusion, we first look at the state of play of current EU cybersecurity law and policy. We then identify gaps in this framework and summarise the gaps identified by a variety of stakeholders. Finally, we formulate policy recommendations for a more connected EU cybersecurity framework.

State of play of the EU cybersecurity framework

Since 2020, the EU has seen a range of cybersecurity legislation emerging or undergoing review. The cybersecurity legislative landscape has become more dynamic and complex than ever, with the IoT increasingly falling within the scope of these instruments.

Cybersecurity legislation and instruments with cybersecurity implications

The NIS Directive (European Parliament and Council 2016) lays down horizontal rules which aim to increase the level of cybersecurity across the EU. It applies to essential services for the economy and society and digital service providers, setting requirements for risk management, information security policy and incident notification. The Directive is under review at the time of writing: the NIS 2 Directive (NIS2) will address evolving cybersecurity needs by expanding the scope (including medical devices, Domain Name System, DNS and others) and reach (e.g. coordinated vulnerability disclosures, setting a common EU cyber-crisis mechanism) of the legislation. The EU Cybersecurity Act (CSA) was adopted in 2019 to strengthen the role of the European Cybersecurity Agency (ENISA) and to create a framework for the common EU cybersecurity certification of information and communications technology products, services and processes. The use of the CSA's certification scheme is voluntary, but it is left at the discretion of member states as to whether they wish to mandate it. The risk is that some member states will introduce mandatory certification and others will not. This could lead to further fragmentation of the single market. Three candidate frameworks are under development, focusing on cloud solutions, ICT products and 5G. The IoT-focused cybersecurity certification is next in line for development.

While horizontal instruments such as the 2022 AI Act proposal or the 2016 General Data Protection Regulation (GDPR) do not lay out specific security standards, the latter requires that 'appropriate technical and organisational measures to ensure a level of security appropriate to the digital risk' are implemented (Art. 32 Security of processing, GDPR). The AI Act proposal in its current agreed text therefore establishes a broad cybersecurity requirement for AI systems, acknowledging the role of cybersecurity in creating resilient AI systems.

In parallel, a range of sector-specific legislation includes cybersecurity requirements. The 2017 MDR lays down resilience, safety and performance requirements for medical devices. However, no reference is provided to other applicable cybersecurity laws, such as the NIS2, or the CSA certification scheme. Alongside the MDR, the Radio Equipment Directive (RED, Directive 2014/53/EU) sets safety standards for wireless devices which transmit radio signals. With the 2022 Delegated Act expanding its scope, it will become possible for the competent national authorities (e.g. national cybersecurity agencies/directorates) to remove IoT products from the market if they do not adhere to the regulation's requirements. As a result, if the legislation fulfils its intention, from 2024 cybersecurity and privacy by design will become conditions for EU market access. Finally, the 2020 Critical Entities Resilience (CER) Directive, aims to improve the physical resilience of critical entities. The entities listed in the NIS will likely be covered under the CER, and the member states can complement this list with the entities they consider critical.

Common Security and Defence Policy

Cyber resilience is also a priority in the EU's Common Security and Defence policy. The new Strategic Compass, adopted in 2022, sets the EU security agenda to 2030. It

proposes several initiatives in the field of cybersecurity, such as furthering the Cyber Diplomatic Toolbox, currently used for cyber sanctions (see how in Cyen 2021); creating a new Hybrid Toolbox and Response Team, bringing together different instruments to detect and respond to a broad range of hybrid threats (including cyber threats); and setting up an EU Cyber Defence Policy to increase the EU's cyber preparedness. Furthermore, in the military field, the EU has launched cyber-related projects as part of its Permanent Structured Cooperation Framework, including the launch of Cyber Rapid Response Teams to improve member states' cooperation in cyber resilience and incident response, as well as the multinational Cyber and Information Domain Coordination Centre for voluntary information exchange between the Member States. EU ministers have also supported the European Commission in establishing a new Emergency Response Fund for Cybersecurity to prepare the EU to face large-scale cyber-attacks (Euractiv 2022).

The proposed EU Cyber Resilience Act

At the time of finalising this article, the Cyber Resilience Act (CRA) was just proposed. The EU recognised that everything placed on the EU market must be 'secure-by-design' as the IoT proliferates (European Commission 2020b). More enforceable rules are required to ensure a common level of cybersecurity throughout the member states. The CRA aims to tackle these issues and establish minimum security requirements in the EU single market. The proposal covers a wide range of products with digital element for their whole life cycle (European Commission 2022b). Its scope is, therefore, quite broad, however, services are not included in the scope. Initially, the Commission planned to cover also ancillary services; any service related to a product without which the product could not function or run. In this case, digital product covers hardware and software products and software that is available independently of hardware (so-called non-embedded software). However, this did not make it into the proposal.

Crucially, the CRA should become a part of the new legislative framework (NLF). Adopted in 2008, the NLF aims to strengthen the internal market by improving market surveillance rules, establishing common accreditation criteria and improving the conformity assessment of products. The EU's product safety legislation, the General Product Safety and the Machinery Directives (published in 2021), which also form part of the NLF, are undergoing review to address cybersecurity needs. The draft proposals require the relevant operators and authorities to consider cybersecurity when designing or manufacturing a product or machine. While the Machinery Directive covers the industrial IoT, most IoT devices will fall under the Product Safety Directive with its new focus on digital products. With the NLF, it is envisaged that digital products, such as connected devices, will be subjected to rather strict compliance regimes, as can already be observed under the GDPR and the AI Act Proposal.

Finally, member states' cybersecurity legislation will be important when new legislation such as the CRA is considered for adoption by the Council of the EU. Experience shows that member states protect/propose national instruments (if mature) and support

EU initiatives when there is no equivalent policy at home. Majority of the member states' only cybersecurity law is the implementation of the NIS Directive and many refer to an industry standard, such as ISO27k . Indeed, the most popular amongst the industry is the information security standard is ISO27001, complemented by the US National Institute of Standards and Technology (NIST) information security framework, both horizontal standards. However, for the IoT use case, a series of new ISO/IEC vertical standards covering the interoperability, design and deployment aspects is becoming available (Cyen 2022a).

Gaps

While the EU has followed an ambitious policy agenda regarding digitalisation and cybersecurity, adopting several policy instruments, gaps remain. For example, the role of the supply chain in improving security, while recognised, is not sufficiently covered by the legislation. In addition, widely used hardware, non-embedded software, digital services and ancillary services are insufficiently covered. Moreover, while the CRA proposal is an improvement, specifically addressing the secure development and vulnerability management, the whole life cycle of a product/service is not covered – for instance, guidance on secure testing, compliance review, secure decommissioning, and logs, incident and crisis management is still missing.

In addition, while EU legislation has started differentiating between the rules according to risk categories (e.g. the NIS approach to important entities and the CRA, AI Act or MDR depending on risk category), we also identify a need to integrate a risk-based approach into the policy-development process. For example, the cybersecurity threat landscape and security risks are not systematically considered when developing digital policies (e.g. the Digital Services and Digital Markets Acts) or enforcement mechanisms.

With regard to the Common Security and Defence Policy, numerous initiatives show that while the EU is following an ambitious agenda to make cybersecurity a priority across the security field, the synergies between defence, investment and cybersecurity policies are limited by a lack of alignment and central coordination of these strategies. Furthermore, the EU's powers in external actions are limited, which raises the question of whether a proper level of cyber defence can be reached on the EU level alone. The EU Hybrid Toolbox partially tackles this issue by focusing on coordinating national and European policies in the field of cyber defence.

There is also a disparity between the cybersecurity capacity in different regions (e.g. north vs. south, big vs. small member states) and the cybersecurity maturity of sectors (e.g. high maturity in fintech and telecommunications vs. less mature in healthcare, energy and construction, to name few). Cybersecurity also depends on external factors such as international security (changing the threat landscape), the economy (investment capacity) and technology (quantum and AI could change the game). As a result, the implementation of EU legislation across the EU is somewhat variable and shows considerable inconsistencies.

Furthermore, we have identified a significant time lapse between objective definition and implementation: just under 10 years usually pass from initiation to effective implementation in companies. Examples include the GDPR, for which the public consultation in preparation for the Commission proposal from 2012 started in 2009 (European Commission 2012), with the final text adopted in 2016, and effective and implemented in companies from 2018. A similar delay was observed in the adoption of the NIS Directive, which was conceptualised in 2012, proposed in 2013, adopted in 2016, effective from 2018 (transposed in national law) and implemented in companies from 2019. As such, every piece of legislation should be designed to address the legislator's objective at least 10 years ahead.

In addition, to understand how to reduce the EU's IoT cybersecurity risk, we need to understand the vulnerabilities. An ENISA Advisory Group report found the lack of security in connected devices to be mostly because the producers of connected devices have no legal obligations regarding cybersecurity standards (ENISA 2019). Furthermore, ENISA has established that IoT devices are often more vulnerable than classical software devices, as their firmware is not regularly updated and/or the hardware does not match the security abilities of the software. The European Commission has also found that a rush to market without due regard for security measures, a lack of cybersecurity experts in product and software development processes, and a lack of economic incentives contribute to the issue (European Commission 2022a).

Stakeholders' views align on what gaps the Cyber Resilience Act could address. The industry (Euroconsumers, Digitaleeurope) is united around the idea of a common EU approach to cyber threats that enables consumers to trust the IoT (Euractiv 2021, Digitaleurope 2022). The EU's 'Better Regulation' toolkit has been mentioned by industry and the Commission itself in the NIS2 as a starting point for creating future-proof effective regulation. The Netherlands supports a horizontal approach, implementing mandatory measures, covering consumer and business-to-business connected products and services across their entire life cycle, targeting the manufacturers and providers of information and communication technology products, processes and services. The European Consumer Protection Organisation demands, specifically, that encryption, authentication and security update standards be improved (BEUC 2022). Scholars have also raised terminological issues: for instance, existing EU legislation applies different meanings to cybersecurity and needs to clarify the difference between resilience and security.

Conclusions

Cyber resilience has been a key EU priority since 2020. EU policymakers have focused on improving critical sectors' cybersecurity (e.g., through the NIS2, CER and CRA) and have introduced cybersecurity in key sectoral legislation (the MDR, the RED, the Machinery Directive, the General Product Safety Regulation, the AI Act). Member states generally follow EU cybersecurity legislation without reinforcing the rules in national legislation.

The EU should lead the work but not reinvent the wheel. Cybersecurity standards could play a critical role in increasing harmonisation, introducing actionable requirements, and increasing legal certainty. For example, several popular process-based information security standards and many new IoT security standards exist. Developed in industry forums, such standards are technology-neutral and future-proof. These are objectives that policymakers should aspire to when designing legislation with cybersecurity impact.

To address the identified gaps, the EU should focus on addressing IoT cybersecurity solutions for products' complete lifecycles. Supply-chain cybersecurity should be consistently taken into account. Industry standards or the CSA certification scheme should be used when new rules are designed. When sector-specific risks arise, sectoral standards should be prioritised. Careful impact analysis, accompanied by a cybersecurity threat analysis and projection, should be integrated into the legislative process at every step.

The specific recommendations for EU policymakers below focus on streamlining the cybersecurity legislation and strengthening the cybersecurity governance and enforcement framework.

A risk-based approach

Inspired by the GDPR's success, the EU should adopt a risk-based approach in future cybersecurity legislation (such as the CRA) to allow sufficient flexibility. Aligning the risk categories with the AI Act is necessary to ensure consistency. The more critical the security risks of the product or services, the more stringent the requirements needed. High-risk products or services should have sectoral legislation or guidance, referencing sector or product-specific standards. Industry standards cover the IoT case. If no industry standards options are available for other sectors, an EU cybersecurity certification framework should be developed to cover the gap. Finally, the requirements should be aligned with the NLF's essential requirements—define the results to be attained or the risks to be dealt with, but do not specify the technical solutions for doing so.

A strong cybersecurity governance and enforcement framework

The NLF could be enhanced to address the EU's cybersecurity needs. The EU needs to update the NLF for it to take a security rather than a safety viewpoint and to expand the NLF's focus from product to 'solution'. In addition, ENISA should support and guide the conformity assessment bodies to play their new role linked to cybersecurity enforcement and supervision.

As per the GDPR model, we should put in place a continuous support and guidance mechanism to make EU cybersecurity legislation effective. We have all the elements necessary but need to define the roles and responsibilities. For instance:

- The NIS cooperation group, coordinated by ENISA, has already delivered helpful guidance for the implementation of the NIS Directive, similar to that provided by the European Data Protection Board for the GDPR. Such implementation guidance provides flexibility through a simplified consultation and publishing cycle, specifically tackling one topic at a time, improving clarity and legal certainty. Policymakers should apply this successful approach to future EU cyber legislation (such as the CRA).
- The NLF could be used to enforce cybersecurity legislation.
- ENISA could play an instrumental role in orchestrating governance and policy development, as the European Data Protection Board does for data protection.
- The newly established EU Cybersecurity Competence Centre (ECCC) could support the implementation of the framework and then the measures through targeted funding and projects (see Cyen – Cybersecurity 2022b) for further information on the ECCC).

An EU cybersecurity impact assessment step in the legislative process

There is a need for an expert analysis and impact assessment to be integrated into the legislative process to ensure new requirements support the objective of improved security for EU citizens and businesses. Just as every company should have a privacy impact assessment for new projects, the EU should have a security impact assessment for any new policy. Better alignment and synergy with the cyber defence agenda and priorities should also be achieved. Existing and new forums could provide expert input to ensure that future and evolving threats and industry best practices are considered in the legislative files. Relevant platforms could be used, such as the NIS Cooperation Group, the ENISA Ad-Hoc Working Groups (for instance on Foresight and Enterprise Security) and the ECCC. A new ENISA expert working group for cybersecurity policy review and coordination should also be established.

References

BEUC. (2022). Cyber resilience act: cybersecurity of digital products and ancillary services. *BEUC response to public consultation*. https://www.beuc.eu/sites/default/files/publications/beuc-x-2022-051_cyber_resilience_act_public_consultation_beuc_position_paper.pdf. Accessed 16 August 2022.

Cyen – Cybersecurity. (2021). Sanctions in cyberspace: The EU and the US diplomatic approaches. *YouTube*, 27 May. https://www.youtube.com/watch?v=Ti7AjuUNCfE. Accessed 29 July 2022.

Cyen (2022a). IoT, how to secure and standardise it?. LinkedIn blogpost. Available at: https://www.linkedin.com/pulse/iot-how-secure-standardise-cyen/?trackingId=DFnFFupp5Zj4FYU6vk%2BKWw%3D%3D. Accessed 1 November 2022

Cyen – Cybersecurity. (2022b). Cybersecurity threats & how the EU joins forces in response (EU Cybersecurity Competence Centre). *YouTube*, minute 6:44-26:07. 20 May. https://www.youtube.com/watch?v=pbtbmOF5zBY&ab_channel=Cyen-cybersecurity Accessed 19 July 2022.

Digitaleurope. (2022). Building blocks for a scalable Cyber Resilience Act. https://www.digitaleurope.org/resources/building-blocks-for-a-scalable-cyber-resilience-act/. Accessed 3 October 2022

ENISA Advisory Group. (2019). *Opinion: Consumers and IoT security*. September. https://www.enisa.europa.eu/about-enisa/structure-organization/advisory-group/ag-publications/final-opinion-enisa-ag-consumer-iot-perspective-09.2019. Accessed 12 July 2022.

Euractiv. (2021). *Internet of Things is missing horizontal cybersecurity standards*. https://www.euractiv.com/section/cybersecurity/news/internet-of-things-is-missing-horizontal-cybersecurity-standards/. Accessed on 15 August 2022.

Euractiv. (2022). *EU countries to call for the establishment of a cybersecurity emergency fund*. 8 March. https://www.euractiv.com/section/cybersecurity/news/eu-countries-to-call-for-the-establishment-of-a-cybersecurity-emergency-fund/. Accessed 1 August 2022.

European Commission. (2020a). EU grants nearly €49 million to boost innovation in cybersecurity and privacy systems. *Press Release*, 20 May.https://digital-strategy.ec.europa.eu/en/news/eu-grants-nearly-eu49-million-boost-innovation-cybersecurity-and-privacy-systems. Accessed 1 August 2022.

European Commission. (2020b).*The EU's cybersecurity strategy for a digital age*. Joint Communication, JOIN (2020) 18 final, 16 December. https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=JOIN:2020:18:FIN. Accessed 30 July 2022.

European Commission. (2021a). Proposal for a Regulation of the European Parliament and of the Council laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and mending certain Union Legislative Acts. COM(2021) 206 final

European Commission. (2022a). *Call for evidence for an impact assessment*. Ref. Ares (2022)1955751.https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13410-Cyber-resilience-act-new-cybersecurity-rules-for-digital-products-and-ancillary-services_en. Accessed on 23 September 2022.

European Commission. (2022b). Proposal For a Regulation of the European Parliament and of the Council on On Horizontal Cybersecurity Requirements For Products with digital elements and amending Regulation (EU) 2019/1020. Cyber Resilience Act. COM(2022) 454 final. https://ec.europa.eu/newsroom/dae/redirection/document/89543. Accessed 23 September 2022.

European Commission. (2022c). National transposition measures communicated by the member states concerning: 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. https://eur-lex.europa.eu/legal-content/EN/NIM/?uri=CELEX:32016L1148. Accessed 1 August 2022.

European Parliament and Council. (2012). Proposal for a Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation, GDPR). COM (2012) 11 final, 25 January. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52012PC0011. Accessed 1 August 2022.

European Parliament and Council. (2016). Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive). OJ L194 (6 July), 1.

European Parliament and Council. (2017). Regulation (EU) 2017/745 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/EEC. (05 April)

European Commission. (2021) Proposal for a Regulation fo the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain union legislative acts. COM(2021) 206 final. (21 April)

European Commission. (2021a) Commission Delegated Regulation (EU) 2022/30 of 29 October 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. (29 October)

Schaffer, A. (2022). The White House wants 11 percent more cybersecurity funding. *Washington Post*, 29 March. https://www.washingtonpost.com/politics/2022/03/29/white-house-wants-11-percent-more-cybersecurity-funding/. Accessed 1 August 2022.

Statista. (2021). Internet of Things (IoT) and non-IoT active device connections worldwide from 2010 to 2025. https://www.statista.com/statistics/1101442/iot-number-of-connected-devices-worldwide/. Accessed 30 May 2022.

Tasheva, I. (2021). Cybersecurity post-COVID-19: Lessons learned and policy recommendations. *European View*. doi:10.1177%2F17816858211059250.

Von der Leyen, U. (2021). *'Strengthening the soul of our Union', State of the Union address, Brussels*, 15 September 2021. https://ec.europa.eu/commission/presscorner/detail/ov/SPEECH_21_4701. Accessed 30 May 2022.

Author biographies

Iva Tasheva is the co-founder and cybersecurity lead at Cyen, a consultancy. She is a member of ENISA's Ad-Hoc Working Group on Enterprise Security and a board member of the DPO Circle.

Ilana Kunkel is a former intern at Cyen. She has a bachelor's degree from Maastricht University in law and public policy and an LLM from Universidade Católica Portuguesa with a focus on tech law.