Int. Cybersecur. Law Rev.
https://doi.org/10.1365/s43439-022-00067-6

# The Cyber Resilience Act: the EU Commission's proposal for a horizontal regulation on cybersecurity for products with digital elements

## An introduction

**Pier Giorgio Chiara**

Received: 25 September 2022 / Accepted: 26 September 2022


**Abstract** The EU Commission presented on 15 September 2022 the proposal for a 'Regulation on horizontal cybersecurity requirements for products with digital elements amending Regulation (EU) 2019/1020' (Cyber Resilience Act, CRA). This long-awaited piece of legislation would complement EU cybersecurity *acquis* by laying down horizontal cybersecurity requirements for all products with digital elements. This article sheds light on the 'horizontal' character of the CRA proposal by highlighting its main pillars. In particular, the contribution takes into account the new set of obligations placed on economic operators, the conformity assessment procedures as well as the market surveillance framework and the interplay with other legislative initiatives, both in the policy area and outside EU cybersecurity law. Against the backdrop of the sectoral regulatory approach adopted thus far by the Commission vis-à-vis cybersecurity requirements for products, horizontal intervention is needed to ensure legal certainty, avoiding duplicative obligations and further market fragmentation.

**Keywords** Cybersecurity · Cyber Resilience Act · EU law · Horizontal legislation · NLF

Pier Giorgio Chiara (✉)
University of Luxembourg, Esch-sur-Alzette, Luxembourg
E-Mail: piergiorgio.chiara@uni.lu

University of Bologna, Bologna, Italy

Published online: 02 November 2022

# Das Cyberresilienzgesetz – Vorschlag der Europäischen Kommission für eine horizontale Verordnung zur Cybersicherheit für Produkte mit digitalen Komponenten

Eine Einführung

## 1 Introduction

Cyberattacks and threats on hardware and software components of products have steadily increased in recent years, not only from a quantitative viewpoint but also in terms of their impact and sophistication [1]. The lack of appropriate cybersecurity in products with digital elements in the Union is due to regulatory and market failures, which jeopardize not only the correct functioning of the Internal Market but also individuals' fundamental rights and safety. Malicious actors can compromise seemingly less critical digital products to disrupt networks and information systems connected to them, amid the increasing digitisation permeating every sector of our societies. Moreover, connected products making up the so-called 'Internet of Things' (IoT) seamlessly interact with the 'physical' world in which they operate, through interconnected systems of sensors and actuators. Therefore, the security of these products is directly linked to safety [2], i.e. the dimension aimed at protecting the integrity of life from the threat of imminent danger [3, p. 372].

From an economic perspective, the market failure in providing optimal cybersecurity standards has two main problem drivers, namely information asymmetries and negative externalities. Firstly, consumers are generally unable to assess the overall level of cybersecurity of digital products and may not be willing to pay for more secure options [4]; secondly, several models analysing the optimal investment level in cybersecurity concluded that the cybersecurity market is characterized by a sub-optimal investment level [5, pp. 34–36].

From a regulatory perspective, the European Union (EU) legal framework appears to be fragmented in relation to cybersecurity requirements for products with digital elements, as the various initiatives taken thus far at Union and member state level[1] partially address the identified problems. In particular, sectoral product safety legislation has been enacted or amended to include cybersecurity essential requirements: Regulation (EU) 2017/745 (MDR)[2], Commission Delegated Regulation (EU) 2022/30 (Radio Equipment Directive Delegated Act)[3], the Machinery Regula-

[1] In the cybersecurity field in particular, eminently characterised by its cross-border nature, policy objectives can hardly be tackled effectively by member state legislation. See [21].

[2] Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC.

[3] 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.

[4] Proposal for a Regulation of the European Parliament and of the Council on machinery products, COM(2021) 202 final.

tion proposal (MR)[4] and the General Product Safety Regulation proposal (GPSR)[5]. This creates legal uncertainty for both manufacturers and users while adding an unnecessary burden on market operators to comply with overlapping requirements for similar types of products.

Against this background, the EU Commission's President Von der Leyen announced in the State of the Union address of 2021 a new 'Cyber Resilience Act' (CRA) to ensure a coherent cybersecurity framework with mandatory requirements for manufacturers of products with digital elements, building on the EU's 2020 Cybersecurity Strategy for the Digital Decade [6], the Council Conclusions of 2 December 2020 [7] and the Resolution of the European Parliament of 10 June 2021 [8]. Eventually, the Commission presented the proposal for a regulation on horizontal cybersecurity requirements for products with digital elements amending Regulation (EU) 2019/1020 (CRA) on 15 September 2022. Art. 114 of the Treaty on the Functioning of the European Union (TFEU) has been identified as the legal basis of the initiative, as it provides for the adoption of measures to ensure the establishing and functioning of the internal market.

This article aims at providing a general overview of the CRA Proposal. In particular, Sect. 2 clarifies the horizontal scope of the newly proposed CRA; Sect. 3 addresses the various obligations of economic operators; Sect. 4 maps out the different conformity assessment rules and Sect. 5 highlights the market surveillance and enforcement framework. Furthermore, Sect. 6 briefly dwells on the interplay between the CRA Proposal and existing or proposed legislation vis-à-vis cybersecurity requirements for products, including the proposal for a Regulation on Artificial Intelligence (AIA)[6], the GPSR proposal, the MR proposal, the RED Delegated Act, the proposal for a revision of the Network and Information Security (NIS) Directive (NIS2 Directive)[7] and Regulation (EU) 2019/881[8]. Finally, Sect. 7 sketches conclusive remarks on the importance of and need for this horizontal legislative initiative.

## 2 The 'horizontal' scope of the Cyber Resilience Act

The proposed Regulation applies "to products with digital elements whose intended or reasonably foreseeable use includes a direct or indirect logical or physical data

[5] 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, COM(2021) 346 final.

[6] Proposal for a Regulation of 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.

[7] Proposal for a directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148, COM(2020) 823 final.

[8] 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).

[9] Art. 2(1) CRA Proposal.

connection to a device or network"[9]. 'Products with digital elements' is thus the axis around which the CRA revolves. The Proposal provides for it a broad definition, i.e. "any software or hardware product and its remote data processing solutions, including software or hardware components to be placed on the market separately"[10].

In the call for evidence for an impact assessment, the Commission used to refer to 'digital products and ancillary services'[11] without specifying in detail what constitutes an 'ancillary service'. In this regard, an early debate emerged amongst stakeholders. On the one hand, Digitaleurope, the leading trade association representing digitally transforming industries in the EU, took the view that the scope of the CRA should not encompass general-purpose ('standalone') software nor 'ancillary services', "both of which function irrespective of a specific tangible product and are not suitable for the same legislative treatment" [9, pp. 7–8]. On the other hand, other industrial and consumers associations such as Eurosmart, BEUC (Bureau Européen des Unions de Consommateurs) and ANEC (European Association for the Co-ordination of Consumer Representation in Standardisation AISBL) consider that the scope of the CRA should be as broad as to cover not only non-embedded software [10, pp. 8–9, 11, pp. 3–5] but also digital cloud services [12, p. 7]—even though, in this latter case, overlaps may occur with the NISD/NIS2 legal framework (see Sect. 6).

The horizontal scope of the Proposal is thus even broader than originally envisaged in the call for evidence. Thus, the definition of 'products with digital elements' mentioned above also extends to software as a separate product from the hardware, as testified by the disjunctive use of the conjunction 'or'. This is confirmed by the reading of recital 46 of the Proposal which explicitly envisages products with digital elements in the form of software. Without dwelling on the legal consequences of considering software as a product—to which vast literature is devoted[12]—as it would be outside of the scope of the present article, the extent to which the CRA covers software-as-a-product, that is, standalone software, shall be further investigated.

The explanatory memorandum of the Proposal starts from the consideration that the "current EU legal framework does not address the cybersecurity of non-embedded software"[13]. To this end, the policy option that has been preferred was the one covering all software: "this option would ensure the setting out of specific horizontal cybersecurity requirements for all products with digital elements being placed or made available on the internal market, and would be the only option covering the entire digital supply chain. Non-embedded software, often exposed to vulnerabilities, would also be covered by such regulatory intervention, thus ensuring a coherent approach towards all products with digital elements, with a clear share of responsibilities of various economic operators"[14].

[10] Art. 3(1) CRA Proposal.

[11] EU Commission, see <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>.

[12] See *inter alia* [22].

[13] Explanatory Memorandum to the CRA proposal, p. 1.

[14] *Ibidem,* p. 7.

However, recital 9 of the Proposal specifies that the CRA would not cover Software-as-a-Service (SaaS), "except for remote data processing solutions relating to a product [...] for which the software is designed and developed by the manufacturer of the product concerned or under the responsibility of that manufacturer, and the absence of which would prevent such a product with digital elements from performing one of its functions". In this sense, it seems that the 'ancillary' perspective is somewhat maintained, as services (SaaS, in this case) may be included if they relate to (i.e., they are designed and developed for) a product with digital elements. Importantly, free and open-source software are excluded from the scope of the Proposal, in order not to hamper innovation or research[15].

As regards other exceptions, the Proposal clarifies that the CRA would not apply to products with digital elements which already fall within the scope of Regulation (EU) 2017/745 (Medical Devices Regulation)[16], Regulation (EU) 2017/746 (Regulation on in vitro diagnostic medical devices) and Regulation (EU) 2019/2144 (Automotive type-approval general regulation)[17], nor would it apply to products with digital elements that have been certified in accordance with Regulation (EU) 2018/1139 (Common rules in civil aviation)[18]. Also excluded from the scope of the CRA are those products with digital elements exclusively developed for national security, military purposes or specifically designed to process classified information[19].

The Proposal hinges on a risk-based approach [13]. In relation to the level of cybersecurity risk related to the product category—determined by the Commission by taking into account several criteria such as the cybersecurity-related functionality, the intended use in sensitive environments or of performing critical functions and the extent of an adverse impact[20], specific products with digital elements can be classified as critical or highly critical if their core functionality falls into those categories[21]. The former category is further divided into class I[22] and class II[23], with class II representing a greater cybersecurity risk, and it is listed in Annex III to the CRA. The latter category can be created in the future by the Commission through the adoption of delegated acts[24].

[15] Recital 10 CRA Proposal.

[16] Whereas the CRA does not cover medical devices, it would cover devices that gather and process also health data not falling under the scope of the MDR. See [23, p. 483]: "with reference to Article 2(1) of the MDR, the threshold between a 'medical' and 'non-medical' device is the "intended purpose": whether the device is intended to be used by the manufacturer, alone or in combination, for one of the listed "specific medical purposes". The recent rise of consumer (well-being, lifestyle) health devices has blurred the borderline between 'medical' and 'non-medical' devices".

[17] Art. 2(2) CRA Proposal.

[18] Art. 2(3) CRA Proposal.

[19] Art. 2(5) CRA Proposal.

[20] Art. 6(2) CRA Proposal.

[21] Art. 6(1) and 6(5) CRA Proposal.

[22] This class of products include *inter alia* identity management systems software and privileged access management software password managers, network traffic monitoring systems, SIEM systems.

[23] This class of products include *inter alia* operating systems, public key infrastructure and digital certificate issuers, firewalls, intrusion detection systems, general purpose microprocessors.

[24] Art. 6(5) CRA Proposal.

The difference between non-critical, critical and highly critical products with digital elements lies in the different conformity assessment procedure they must undergo. Whereas critical products shall be subject to the specific conformity assessment procedures referred to in Art. 24(2) and (3) CRA[25] (see Sect. 4), manufacturers of highly critical products are required to obtain an EU cybersecurity certificate under a European cybersecurity certification scheme to demonstrate conformity with the essential requirements set out in Annex I, or parts thereof[26].

## 3 The obligations of economic operators

Another aspect that shall be discussed in relation to the horizontal scope of the Proposal is the wide coverage of the CRA's obligations in terms of the economic operators impacted by the Regulation: from manufacturers up to distributors and importers, as adequate for their responsibilities on the supply chain, a wide array of stakeholders will have to comply with the new set of rules. In this respect, the new approach in EU cybersecurity law of including the entire value chain of products with digital elements into its scope should be underlined. The relationships between market operators in the supply chain and due diligence have primarily been contractual, whereas now manufacturers shall exercise due diligence when integrating components sourced from third parties in products with digital elements[27].

Three main general conditions regulate the placing on the market of products with digital elements: i) they are properly installed, maintained, used for their intended purpose and, where applicable, updated[28]; ii) they have been designed, developed and produced in accordance with the essential requirements laid down in Sect. 1 of Annex I[29]; and, iii) the processes put in place by the manufacturer comply with the essential requirements set out in Sect. 2 of Annex I[30].

Pursuant to the essential requirements of Sect. 1, Annex I products with digital elements shall be designed, developed and produced to ensure an appropriate level of cybersecurity based on the risks; shall be delivered without any known exploitable vulnerabilities; shall be delivered with a secure by default configuration; shall ensure protection from unauthorised access by appropriate control mechanisms; shall protect the confidentiality of processed personal or other data by means of state-of-the-art encryption, etc.

Conversely, Sect. 2 of Annex I lays down essential requirements in terms of the processes put in place by manufactures. They include: the identification and documentation of vulnerabilities and components contained in the product, including by drawing up a software bill of materials in a commonly used and machine-readable format covering at the very least the top-level dependencies of the product; the mit-

[25] Art. 6(4) CRA Proposal.

[26] Art. 6(5) CRA Proposal.

[27] Art. 10(4) CRA Proposal.

[28] Art. 5, point (1) CRA Proposal.

[29] Art. 10(1); Art. 5, point (1) CRA Proposal.

[30] Art. 5, point (2) CRA Proposal.

igation of vulnerabilities without delay, including by providing security updates; the application of effective and regular tests and reviews of the security of the product; the public disclosure of information about fixed vulnerabilities, once a security update has been made available, etc.

In line with the risk-based spirit of the Proposal, manufacturers shall undertake an assessment of the cybersecurity risks related to a product category whose outcome must be taken into account during the planning, design, development, production, delivery and maintenance phases of the product with digital elements, for the purpose of complying with the obligation to place a product on the market in accordance with the essential requirements of Sect. 1, Annex I[31]. The risk assessment shall be included in the technical documentation as set out in Art. 23 and Annex V[32].

Manufacturers also have several documentation obligations vis-à-vis the handling vulnerabilities and information provided by third parties[33]. In particular, Art. 23 specifies the content of the technical documentation to be drawn up by the manufacturer before the product is placed on the market and to be kept at the disposal of the market surveillance authorities for ten years after the product has been placed on the market[34]. Thus, in relation to the cooperation with market authorities, manufacturers shall also: i) provide that authority with all the information necessary to demonstrate the conformity with Annex I essential requirements, and cooperate on any measurers taken to eliminate the cybersecurity risks posed by the product[35]; and, ii) inform the authority about the cessation of its operations with the consequence of not being able to comply with the obligations of the Regulation[36].

Moreover, manufacturers shall ensure that products with digital elements are accompanied by the information and instructions set out in Annex II, in an electronic or physical form, in a clear, understandable, intelligible and legible language[37]. The instructions and information may include the EU declaration of conformity[38].

Article 11 laying down the reporting obligations of manufacturers adopts a centralised approach. The manufacturer shall, without undue delay and in any event within 24 h of becoming aware of it, notify to ENISA (European Union Agency for Cybersecurity) any actively exploited vulnerability contained in the product, including the details and any mitigating measures taken. ENISA shall, without undue delay, unless for justified cybersecurity risk-related grounds [14], forward the notification to the Computer Security Incident Response Team (CSIRT) designated for the purposes of coordinated vulnerability disclosure under the NIS2 framework. In the event of an incident occurring to the product with digital elements, manufacturers also have reporting duties to: i) users of the product who, where applicable, shall be told about corrective measures to be deployed to mitigate the impact of

[31] Art. 10(2) CRA Proposal.

[32] Art. 10(3) CRA Proposal.

[33] Art. 10(5) CRA Proposal.

[34] Art. 10(8) CRA Proposal.

[35] Art. 10(13) CRA Proposal.

[36] Art. 10(14) CRA Proposal.

[37] Art. 10(10) CRA Proposal.

[38] Art. 10(11) CRA Proposal.

the incident[39]; ii) the person or entity maintaining the component—integrated in the product—affected by a vulnerability identified by the manufacturer[40]. This is yet another example of how the CRA would take into account supply chain cybersecurity.

Finally, Articles 12, 13 and 14 place obligations on economic operators other than the manufacturer, that is, authorised representatives, importers and distributors, respectively. Importantly, if the importer or distributor i) places a product on the market under its name or trademark or ii) carries out a substantial modification of the product, then the importer or the distributor shall be considered a manufacturer and therefore shall be subject to the obligations of the manufacturer set out in Articles 10 and 11(1), (2), (4) and (7)[41]. Yet, the same applies to any natural or legal person who carries out a substantial modification.

This begs therefore the question of what a substantial modification is under the CRA. According to Art. 3, point (31) CRA, 'substantial modification' "means a change to the product with digital elements following its placing on the market, which affects the compliance of the product with digital elements with the essential requirements set out in Sect. 1 of Annex I or results in a modification to the intended use for which the product with digital elements has been assessed".

## 4 Conformity with the essential requirements

The Cyber Resilience Act Proposal is aligned with the principles of the New Legislative Framework (NLF) in product safety legislation[42]. The NLF, consistent with the so-called 'New Approach' of the 1980s, pivots on laying down only high-level essential requirements in terms of health and safety that products have to meet in order to be placed on the Internal Market; these requirements are then detailed by harmonised technical standards drafted by European Standardisation Organisations (ESOs, i.e. ETSI, CEN, CENELEC) on the basis of a standardisation request by the Commission [15, pp. 16–17].

Products in conformity with harmonised standards, or parts thereof, the references of which have been published in the *Official Journal of the European Union,* shall be presumed to be in conformity with the essential requirements of the Directives and Regulations of the NLF. The same applies to the Cyber Resilience Act (Art. 18). Such presumption of conformity also extends to products and processes put in place by the manufacturer for which an EU statement of conformity or certificate has been issued under a European cybersecurity certification scheme adopted as per Regu-

[39] Art. 11(4) CRA Proposal.

[40] Art. 11(7) CRA Proposal.

[41] Art. 15 CRA Proposal.

[42] 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, the latter being amended by the CRA. See [24, pp. 9–10].

[43] Art. 18(3) CRA Proposal.

lation (EU) 2019/881[43]. In this regard, the Commission may adopt implementing acts to specify the schemes that can be used to demonstrate conformity the essential requirements of Annex I and whether a cybersecurity certificate eliminates the obligation of a manufacturer to carry out a third-party conformity assessment for the corresponding requirements[44].

Importantly, if harmonised standards do not exist, are insufficient or whether there are undue delays in the standardisation procedure or the Commission request has not been accepted by the ESOs, the Commission may, by means of implementing acts, adopt common specifications[45] that can be used to demonstrate conformity with the essential requirements of Annex I, to the extent those common specifications cover those requirements[46].

The EU declaration of conformity shall be drawn up by manufacturers as part of the documentation duties under Art. 10(7). It states that the fulfilment of the applicable essential requirements set out in Annex I has been demonstrated[47]. Annex IV charts out the structure of the EU declaration of conformity model: in particular, it must contain the elements specified in the relevant conformity assessment procedures, it shall be continuously updated[48] and—if a product with digital elements is subject to more than one Union act requiring an EU declaration of conformity—it shall contain the identification of the Union acts concerned[49].

The manufacturer shall perform a conformity assessment of the product by following one of the procedures set out in Annex VI, including: (a) the internal control procedure (based on module A of Decision 768/2008/EC); or (b) the EU-type examination procedure (based on module B) followed by conformity to EU-type based on internal production control (based on module C); or (c) conformity assessment based on full quality assurance (based on module H)[50]. As mentioned above in Sect. 2, manufacturers of critical products of class I and II shall use for the compliance either the EU-type examination procedure (based on module B) followed by conformity to EU-type based on internal production control (based on module C) or conformity assessment based on full quality assurance (based on module H)[51]. With specific regard to the products pertaining to class I, such procedures shall be carried out *if* the manufacturer has not applied or *has applied only in part* harmonised standards, common specifications or European cybersecurity certification schemes; or where such harmonised standards, common specifications or European cybersecurity certification schemes do not exist[52].

[44] Art. 18(4) CRA Proposal.

[45] Art. 19 CRA Proposal.

[46] Art. 18(2) CRA Proposal.

[47] Art. 20(1) CRA Proposal.

[48] Art. 20(2) CRA Proposal.

[49] Art. 20(3) CRA Proposal.

[50] Art. 24(1) CRA Proposal.

[51] Art. 24(2) and (3) CRA Proposal.

[52] Art. 24(2) CRA Proposal.

Before placing the product with digital elements on the market, the CE marking shall be affixed visibly, legibly and indelibly to the product[53] and it follows the general principles set out in Article 30 of Regulation (EC) No 765/2008[54].

Chapter IV of the Proposal then sets out the procedural framework vis-à-vis the interactions with national conformity assessment bodies (notified bodies). The Proposal, consistent with the NLF, leaves the responsibility with the Member States for designating a notifying authority that shall be responsible for setting up and carrying out the necessary procedures for the assessment and notification of conformity assessment bodies and monitoring of notified bodies[55].

## 5 Market surveillance and enforcement

In accordance with Regulation (EU) 2019/1020, which applies to the products with digital elements in scope of the CRA[56], national market surveillance authorities (MSAs)—designated by Member States—carry out market surveillance in the territory of that Member State. Member States may designate any existing or new authority for the purpose of ensuring the effective implementation of the CRA, including national competent authorities under the NIS2 and the Cybersecurity Act (CSA)[57]. However, for products with digital elements in the scope of the CRA, which are classified as well as high-risk AI systems according to the Artificial Intelligence Act (AIA), the MSAs designated for the purposes of the AIA shall be the authorities responsible for market surveillance activities required under the CRA[58].

MSAs under the CRA shall cooperate with other market surveillance authorities designated on the basis of other Union harmonisation legislation for other products, with the national cybersecurity certification authorities designated under the CSA and, as appropriate, with data protection authorities. In this respect, joint activities between MSAs can be carried out, and may even be proposed by the Commission or ENISA, with the aim of ensuring cybersecurity and protection of consumers with respect to specific products with digital elements placed or made available on the market[59]. Moreover, MSAs may decide to conduct simultaneous coordinated control actions ("sweeps") of particular products with digital elements, or categories thereof, to check compliance with or to detect infringements to the CRA[60]. Unless otherwise decided by the MSAs concerned, these sweeps shall be coordinated by the Commission.

[53] Art. 22(1) CRA Proposal. For products with digital elements which are in the form of software, the CE marking shall be affixed either to the EU declaration of conformity referred to in Article 20 or on the website accompanying the software product.

[54] Art. 21 CRA Proposal.

[55] Art. 26 CRA Proposal.

[56] Art. 41 CRA Proposal.

[57] Recital 55 CRA Proposal.

[58] Art. 41(10) CRA Proposal.

[59] Art. 48 CRA Proposal.

[60] Art. 49 CRA Proposal.

MSAs shall report to the Commission on an annual basis the outcomes of relevant market surveillance activities. These include evaluations of products in respect of their compliance with the requirements of the CRA, which shall be carried out if the MSA has sufficient reasons to consider that the products concerned present a significant cybersecurity risk[61]. Where the product does not comply with the Regulation, the MSA shall without delay require the relevant operator to take all appropriate corrective actions to bring the product into compliance with those requirements, to withdraw it from the market, or to recall it within a reasonable period[62]. If the manufacturer does not take the adequate corrective actions within the timeframe given by the authority, the MSA shall take measures to prohibit or restrict that product being made available on its national market, to withdraw it from that market or to recall it[63]. The Commission may initiate MSA evaluations pursuant to Art. 43 and, in exceptional circumstances—which include reasons to consider that no effective measures have been taken by the relevant market surveillance authorities, may request ENISA to carry out an evaluation of compliance[64]. Accordingly, corrective or restrictive actions may be adopted by the Commission at Union level via implementing acts.

The Proposal delegates to the Member States the power to set rules on penalties—which shall be effective, proportionate and dissuasive—applicable to infringements of the CRA[65]. However, the discretion of Member states is relative: i) non-compliance with the essential cybersecurity requirements of Annex I and the obligations set out in Articles 10 and 11 shall be subject to administrative fines of up to 15M EUR or, if the offender is an undertaking, up to 2.5% of its total worldwide annual turnover for the preceding financial year, whichever is higher[66]; ii) non-compliance with any other obligations under this Regulation shall be subject to administrative fines of up to 10M Euro or, if the offender is an undertaking, up to 2% of its total worldwide annual turnover[67]; and, iii) supply of incorrect, incomplete or misleading information to notified bodies and market surveillance authorities in reply to a request shall be subject to administrative fines of up to 5M Euro or, if the offender is an undertaking, up to 1% of its total worldwide annual turnover[68]. Member States shall notify the Commission of those rules and measures without undue delay[69].

[61] Art. 43(1) CRA Proposal.

[62] *Ibidem.*

[63] Art. 43(4) CRA Proposal.

[64] Art. 45 CRA Proposal.

[65] Art. 53(1) CRA Proposal.

[66] Art. 53(3) CRA Proposal.

[67] Art. 53(4) CRA Proposal.

[68] Art. 53(5) CRA Proposal.

[69] Art. 53(2) CRA Proposal.

## 6 Interplay between the CRA and other Union policies

As already stated in the Introduction, the CRA is intended to close a gap in EU legislation with regard to cybersecurity requirements for products; so far, the governance approach endorsed by the Commission has been 'vertical', that is, sector-specific [16]. The CRA is the remaining piece of the jigsaw that would create an interface between all the legal acts addressing products cybersecurity, either directly or indirectly, such as the existing and proposed Directives and Regulations of product safety legislation, the AIA, the CSA, the Delegated Regulation (EU) 2022/30 and the NIS2.

The interaction between the CRA and other Union legal acts imposing cybersecurity requirements for products with digital elements is regulated by Art. 2(4) of the Proposal. This provision can be interpreted as a rule of prevalence as it lays down the criteria by which other EU legal frameworks addressing all or some of the risks covered by the essential requirements set out in Annex I to the CRA may in fact prevail over the CRA. Thus, the application of the CRA may be limited or excluded if the sectoral rules applying to the products achieve the same level of protection as the one provided for by the CRA and if such prevalence is consistent with the overall regulatory framework applying to those products. The Commission may specify, through delegated acts, whether such limitation or exclusion is necessary, the concerned products and applicable rules, as well as the scope of the limitation.

The following sections will map out some preliminary remarks related to the interplay between the Cyber Resilience Act Proposal and other Union legal acts without dwelling on the identified legal challenges too extensively, as they will form the subject matter of another article of this thematic edition of International Cybersecurity Law Review.

### 6.1 Interplay between the CRA and the Artificial Intelligence Act Proposal

Products falling under the scope of the CRA which are eventually classified as high-risk AI systems according to Art. 6 of the AI Act Proposal shall comply with the essential requirements set out in Annex I to the CRA[70]. When those high-risk AI systems fulfil CRA's essential requirements, they shall be deemed compliant with the cybersecurity requirements set out in Article 15 of the AI Act Proposal in so far as those requirements are covered by the EU declaration of conformity, or parts thereof, issued under the CRA[71].

Conversely, having regard to the conformity assessment procedures relating to the cybersecurity essential requirements of said products, Art. 43 of the AI Act prevails over the respective provisions of the CRA[72], as previously addressed by Sect. 4. As a consequence, the notified bodies that control the conformity of high-risk AI systems under the AI Act are entitled to control the conformity with the essential requirements set out in Annex I to the CRA. However, if high-risk AI

[70] Art. 8(1) CRA Proposal.

[71] *Ibidem.*

[72] Art. 8(2) CRA Proposal.

systems are also qualified as *critical* products under the CRA, then they are subject to the conformity assessment rules of the CRA[73].

### 6.2 Interplay between the CRA and the General Product Safety Regulation Proposal

Article 7 of the CRA aims at clarifying the interface between the CRA and the General Product Safety Regulation. The latter will apply as *lex generalis* to non-harmonised products and to the harmonised consumer products for the aspects that are not covered by harmonised legislation[74]. Art. 7 CRA reads as follows:

> "*By way of derogation from Article 2(1), third subparagraph, point (b), of Regulation [General Product Safety Regulation] where products with digital elements are not subject to specific requirements laid down in other Union harmonisation legislation within the meaning of [Article 3, point (25) of the General Product Safety Regulation], Chapter III, Section 1, Chapters V and VII, and Chapters IX to XI of Regulation [General Product Safety Regulation] shall apply to those products with respect to safety risks not covered by this Regulation*".

A combined reading of recital 28 CRA and the relevant articles of the GPSR may help disentangle the rather convoluted drafting of this provision. Thus, recital 28 clarifies that products with digital elements might pose other safety risks that are not related to cybersecurity. Those risks are regulated by other relevant Union product safety legislation. If no other harmonised Union legislation is applicable, they should be subject to the GPSR legal framework, consistent with its role of 'safety net'. On the other hand, Article 2(1) GPSR mandates that where products are within the scope of Union product safety legislation, the rules laid down by the GPSR shall apply only to the aspects and risks not covered by those requirements; in particular, Chapter III, Sect. 1, Chapters V and VII, Chapters IX–XI GPSR shall not apply.

According to recital 28 CRA, the derogation from the general rule prescribed by Art. 2(1) GPSR finds its rationale in the targeted nature of the Cyber Resilience Act which covers only cybersecurity-related aspects without addressing general health and safety requirements as the legal acts of EU product legislation. Therefore, the legislator deemed it necessary to extend the coverage of Chapter III, Sect. 1, Chapters V and VII, and Chapters IX–XI GPSR to products with digital elements with respect to safety risks not covered by the CRA.

[73] Article 8(3) CRA Proposal.

[74] 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.

### 6.3 Interplay between the CRA and the Machinery Regulation Proposal

The interface between the Cyber Resilience Act and the Machinery Regulation Proposal is regulated by Art. 9 CRA. It regulates specific aspects of the interplay between the conformity assessments under the two legal instruments. In particular, where machinery products are products with digital elements within the meaning of the CRA and for which an EU declaration of conformity has been issued on the basis of the CRA shall be deemed to be in conformity with the essential health and safety requirements set out in Annex III, Sections 1.1.9 and 1.2.1[75] to the Machinery Regulation proposal.

### 6.4 Interplay between the CRA and the RED Delegated Act

Delegated Regulation (EU) 2022/30 was adopted on 29 October 2021 with a view to specifying to which categories or classes of radio equipment the essential requirements set out in Article 3(3) points (d) (network harm and misuse of network resources), (e) (personal data protection and privacy) and (f) (fraud) of Directive 2014/53/EU on radio equipment (RED) apply.

Importantly, the essential requirements laid down by the CRA include all the elements of the essential requirements referred to in Article 3(3) points (d), (e) and (f) of the RED[76]. Moreover, CRA's essential requirements are also aligned with the objectives of the requirements for specific harmonised standards included in the standardisation request of the Commission to the European Standardisation Organisations to prove conformity with the RED's abovementioned requirements[77].

From the above, it can be concluded that content and objectives of the RED Delegated Act completely overlap with the Cyber Resilience Act Proposal. Indeed, recital 15 CRA explicitly envisages the possibility to repeal or amend Delegated Regulation (EU) 2022/30. If that was the case, the Commission and ESOs "should take into account the standardisation work carried out in the context of Commission Implementing Decision C(2022)5637 on a standardisation request for the RED Delegated Regulation 2022/30 in the preparation and development of harmonised standards to facilitate the implementation of this Regulation"[78].

### 6.5 Interplay between the CRA and the NIS2 Directive

Given the general and introductory scope of the present article, this section casts light on the CRA provisions that provide an interface with the NIS2 Directive without going into a detailed critical analysis of the potential legal challenges stemming from the application of the two frameworks.

[75] As regards protection against corruption and safety and reliability of control systems.

[76] Recital 15 CRA Proposal.

[77] *Ibidem*.

[78] *Ibidem*.

The NIS2 Directive, which will repeal the NIS Directive[79], seeks to modernise the existing EU cybersecurity legal framework while addressing several weaknesses that prevented the NIS Directive—the first piece of EU-wide legislation on cybersecurity—to unlock its full potential. In particular, it aims at ensuring a high level of cybersecurity of services provided by essential and important entities [17]. For the purpose of this article, three areas of interplay are taken into account. They regard: i) the scope of the legal acts; ii) the rules regulating supply chain relationships; and, iii) the reporting of incidents and vulnerabilities.

Software-as-a-service is, with some exceptions, outside the scope of the CRA. NIS2 would therefore complement the CRA by covering cloud computing services and cloud service models, such as SaaS, as all entities providing cloud computing services in the Union that meet or exceed the threshold for medium-sized enterprises fall in the scope of that Directive[80]. Moreover, a criterion that shall be taken into account by the Commission when determining the categories of highly critical products is the fact that a category of products with digital elements is used or relied upon by the essential entities within the meaning of NIS2 or will have potential future significance for the activities of these entities.

Also, the CRA would effectively complement the NIS framework by ensuring the prerequisites for a strengthened supply chain security [16, p. 12]. [81]. Thus, the compliance of NIS2 entities vis-à-vis the supply chain requirements under Art. 18(2)(d), 18(3) and 19 of the NIS2 Proposal would be facilitated by ensuring that the products with digital elements that essential and important entities use in providing their services are designed and manufactured according to state-of-the-art cybersecurity controls. Moreover, the life-cycle approach of the CRA assures that NIS2 entities would have access to timely security updates for such products[82]. In particular, CRA's essential requirements should be without prejudice to the EU coordinated risk assessments of critical supply chains pursuant to Art. 19 NIS2 Proposal, which take into account both technical and non-technical risk factors[83].

A further area of intersection is represented by the reporting duties. As seen in Sect. 3, the reporting obligations of manufacturers primarily concerns the actively exploited vulnerabilities and any incident having impact on the security of the product with digital elements (Art. 11 CRA). The centralised model of governance of the CRA places ENISA at the core of the procedural framework of these notifications. Against the background of the incidents and vulnerabilities reporting duties of essential and important entities under the NIS2, it will be crucial ensuring an efficient and timely communication between ENISA and the single point of contact of the Member States concerned, with respect to the incidents[84], and the CSIRT designated

[79] 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, OJ L 194, 19.07.2016.

[80] Recital 9 CRA Proposal.

[81] Explanatory Memorandum to the CRA Proposal, p. 7.

[82] Recital 11 CRA Proposal.

[83] Recital 33 CRA Proposal.

[84] Art. 11(1) CRA Proposal.

for the purposes of coordinated vulnerability disclosure in accordance with Art. 6 of the NIS2 Proposal[85]. The inclusion of the European cyber crisis liaison organisation network (EUCyCLONe) established by Art. 14 NIS2 Proposal within this coordinated framework[86] suggests the will to build a consistent European ecosystem of digital security and resilience.

### 6.6 Interplay between the CRA and the Cybersecurity Act

The CRA Proposal aims at exploiting synergies with the CSA mainly with regard to the conformity assessment procedure. Art. 18(3) and (4) CRA lay down the interface between the two legal frameworks with a view to promoting the European cybersecurity certification schemes (ECCS) and facilitating the assessment of conformity of products with digital elements—if covered by an EU statement of conformity or certificate under a ECCS pursuant to Regulation (EU) 2019/881.

The Commission may specify, via implementing acts: i) the ECCSs that can be used for the presumption of conformity with CRA's essential requirements; ii) if a cybersecurity certificate issued under such schemes eliminates the obligation of a manufacturer to carry out a third-party conformity assessment for the corresponding requirements[87]. Moreover, the Commission is empowered to adopt delegated acts, in accordance with Art. 50 CRA, to specify categories of highly critical products with digital elements for which the manufacturers shall be required to obtain a certificate under a ECCS to demonstrate conformity with the essential requirements set out in the CRA[88].

Finally, it is interesting to note that recital 39 of the CRA Proposal seems to carve out a benchmark role for the CRA with regard to future ECCSs: "the need for new European cybersecurity certification schemes for products with digital elements should be assessed in the light of this Regulation. Such future European cybersecurity certification schemes covering products with digital elements should take into account the essential requirements as set out in this Regulation and facilitate compliance with this Regulation".

## 7 Conclusion

Harmonised cybersecurity rules and joint action at EU level are the most efficient way to increase the level of trust among users, the attractiveness of products with digital elements with the CE marking and the overall level of cyber resilience. The CRA would benefit the economic operators of the internal market by providing legal certainty and achieving a level playing field for vendors of hardware and software products. This atypical legal act in EU product safety legislation, covering only cybersecurity-related aspects for a very wide category of products without taking

[85] Art. 11(2) CRA Proposal.

[86] Art. 11(3) CRA Proposal.

[87] Art. 18(4) CRA Proposal.

[88] Art. 6(5) CRA Proposal.

into account broader health and safety issues, justifies the instrument of regulation from a policy viewpoint as it would more effectively address the problems identified.

Moreover, the CRA would contribute to the on-going process of shaping an EU concept of cybersecurity [18]. Cybersecurity can thus no longer be reduced to the mere technical protection goals of IT security [19]; it has progressively developed into a social, economic and multidisciplinary challenge. More specifically, connected products expand the *perimeter* of the values and assets that need to be protected. Risk factors and threats in today's IoT hyper-connected digital environment go beyond the technological infrastructure of information systems, networks and the underlying information. An attack could also infringe individuals' fundamental rights, impair physical safety and, as much as the critical infrastructure is concerned, have serious consequences for communities, institutions and businesses.

This perspective, defined elsewhere as '*infraethical*" [20], is acknowledged by the CRA Proposal: "by protecting consumers and organisations from cybersecurity risks, the essential cybersecurity requirements laid down in this Regulation, are also to contribute to enhancing the protection of personal data and privacy of individuals"[89]. In other words, cybersecurity can also be conceived as an *instrumental* value necessary to uphold *fundamental* values, such as fundamental rights and liberties and physical safety.

**Acknowledgements** 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

1. ENISA (2020to) ENISA Threat Landscape 2021. https://doi.org/10.2824/324797
2. Vedder A (2020) Safety, security and ethics. In: Vedder A, Schroers J, Ducuing C, Valcke P (eds) Security and law. Intersentia, Cambridge, Antwerp, Chicago, pp 11–26
3. Durante M (2019) Safety and security in the digital age. Trust, algorithms, standards, and risks. In: Berkich D, D'Alfonso MV (eds) On the cognitive, ethical, and scientific dimensions of artificial intelligence, vol 134. Springer, Berlin Heidelberg, pp 371–383
4. Blythe JM, Johnson SD, Manning M (2020) What is security worth to consumers? Investigating willingness to pay for secure Internet of Things devices. Crime Sci 9(1):1–9. https://doi.org/10.1186/S40163-019-0110-3/FIGURES/3
5. (2021) Wavestone—CEPS—CARSA—ICF, "Study on the need of Cybersecurity requirements for ICT products—No. 2020-0715: Final Study Report," Brussels. https://digital-strategy.ec.europa.eu/en/library/study-need-cybersecurity-requirements-ict-products. Accessed 17 Sept 2022

[89] Recital 17 CRA Proposal.

6. European Commission and the High Representatitve 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
7. Council of the European Union (2020) Council conclusions on the cybersecurity of connected devices. https://data.consilium.europa.eu/doc/document/ST-13629-2020-INIT/en/pdf. Accessed 17 Sept 2022
8. European Parliament (2021on) European Parliament resolution of 10 June 2021 on the EU's Cybersecurity Strategy for the Digital Decade (2021/2568(RSP)). https://www.europarl.europa.eu/doceo/document/TA-9-2021-0286_EN.html. Accessed 19 Sept 2022
9. Digitaleurope (2022) Building blocks for a scalable cyber resilience act. https://www.digitaleurope.org/wp/wp-content/uploads/2022/05/Building-blocks-for-a-scalable-Cyber-Resilience-Act.pdf. Accessed 19 Sept 2022
10. Eurosmart (2022) Cyber Resilience Act (CRA)—new cybersecurity rules for digital products and ancillary services. https://www.eurosmart.com/cyber-resilience-act-cra-new-cybersecurity-rules-for-digital-products-and-ancillary-services/
11. ANEC (2022) ANEC response to EC Call for evidence for an impact assessment on the cyber resilience act (CRA) initiative. https://www.anec.eu/images/Publications/position-papers/Digital/ANEC-2022-DIGITAL-CYBER-006.pdf. Accessed 21 Sept 2022
12. BEUC (2022) Cyber resilience act: cybersecurity of digital products and ancillary services—BEUC response to public consultation. https://www.beuc.eu/publications/beuc-x-2022-051_cyber_resilience_act_public_consultation_beuc_position_paper.pdf. Accessed 22 Sept 2022
13. De Gregorio G, Dunn P (2022) The European risk-based approaches: connecting constitutional dots in the digital age. Common Mark Law Rev 59(2):473–500. https://doi.org/10.54648/COLA2022032
14. Schmitz S, Schiffner S (2021) Responsible vulnerability disclosure under the NIS 2.0 proposal. J Intellect Prop Inf Technol Electron Commer Law 12(5):448–457 (https://www.jipitec.eu/issues/jipitec-12-5-2021/5495)
15. Hofmann HCH (2016) European regulatory Union? The role of agencies and standards. In: Koutrakos P, Snell J (eds) Research handbook on the EU's internal market. Elgar Publishing, Cheltenham, pp 1–20. https://doi.org/10.4337/97817834781O1.00029
16. Chiara PG (2022) The IoT and the new EU cybersecurity regulatory landscape. Int Rev Law Comput Technol. https://doi.org/10.1080/13600869.2022.2060468
17. Schmitz-Berndt S (2021) Cybersecurity is gaining momentum—NIS 2.0 is on its way. Eur Data Prot Law 7(4):580–586. https://doi.org/10.21552/edpl/2021/4/14
18. Papakonstantinou V (2022) Cybersecurity as praxis and as a state: the EU law path towards acknowledgement of a new right to cybersecurity? Comput Law Secur Rev 44:105653. https://doi.org/10.1016/J.CLSR.2022.105653
19. Veale M, Brown I (2020) Cybersecurity. Internet Policy Rev 9(4):1–22. https://doi.org/10.14763/2020.4.1533
20. Chiara PG (2021) The balance between security, privacy and data protection in IoT data sharing: a critique to traditional 'security&privacy' surveys. Eur Data Prot Law Rev 7(1):18–30. https://doi.org/10.21552/EDPL/2021/1/6
21. Schmitz-berndt S, Chiara PG (2022) One step ahead: mapping the Italian and German cybersecurity laws against the proposal for a NIS2 directive. Int Cybersecur Law Rev. https://doi.org/10.1365/s43439-022-00058-7
22. Wagner G (2022) Software as a product. In: Lohsse S, Schulze R, Staudenmayer D (eds) Smart products: Münster colloquia on EU law and the digital economy VI. Nomos, pp 157–179. https://doi.org/10.5771/9783748929772-157
23. Rak R (2021) Internet of healthcare: opportunities and legal challenges in Internet of things-enabled telehealth ecosystems. In: 14th Int. Conf. Theory Pract. Electron. Gov, pp 481–484. https://doi.org/10.1145/3494193
24. European Commission (2016) The 'Blue Guide' on the implementation of EU products rules 2016 (2016/C 272/01)," Off. J. Eur. Union. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016XC0726(02)&from=EN%0Ahttp://ec.europa.eu/DocsRoom/documents/18027/