INTERSECT POLICY BRIEF 1

CYBER RESILIENCE ACT PROPOSAL

Date 15/06/2023

Authors Suzanne Nusselder

Pratham Ajmera

Tilburg University

Understanding Society

Publication

Tilburg Institute for Law, Technology, and Society (TILT)

www.tilt.nl

INTERSECT is funded by the National Research Council (Grant no. NWA.1160.18.301)

Contact

Suzanne Nusselder

S.C.Nusselder@tilburguniversity.edu

1 The Reason behind the Cyber Resilience Act Proposal

The Internet of Things (IoT) has been on the EU's regulatory radar for a while. The European Commission made it an integral part of its 2020 Cybersecurity Strategy,[1] identifying an "Internet of Secure Things" as crucial to providing for secure infrastructures and services across the EU.[2] One of the avenues through which it sought to do so was determining new horizontal rules to improve products and associated service security on all connected products in the Internal Market,[3] a measure intended to harmonise ongoing initiatives that were more sectoral in nature, resulting in the Commission proposing a 'Regulation on horizontal cybersecurity requirements for products with digital elements amending Regulation (EU) 2019/1020' – the Cyber Resilience Act (CRA)[4] – in September 2022.

The CRA is intended to address two major problems affecting products on the internal market: a generally low level of existing cybersecurity for connected devices, and a lack of information among users, preventing them from choosing among available products accurately.[5] To remedy this situation and mitigate the negative impact of cyber-attacks on the internal market, the Commission laid down two main objectives: fostering the development of secure products which have fewer vulnerabilities when placed on the market and are adequately supported throughout their life-cycle, and creating conditions allowing users to choose and use IoT products based on their cybersecurity properties.[6] Specifically, the Commission's proposal for a CRA aims at achieving the following goals:

1. promoting the security of IoT products since their design and development and throughout their whole life cycle;
2. ensuring a coherent cybersecurity framework, facilitating compliance for hardware and software producers;
3. enhancing the transparency of security properties of IoT products; and
4. enabling businesses and consumers to use IoT products securely.[7]

The existing EU cybersecurity framework is comprised of several different instruments that address cybersecurity from different angles[8] but lacks horizontal cybersecurity requirements common to all products with digital elements, hence not covering the entire supply chain. According to the Commission, a more harmonised approach is necessary to fill in the gaps left by existing legislation.[9] The argument for Joint action at EU level was also bolstered by the cross-border nature of cybersecurity, and by the necessity to avoid a fragmented market based on differing national rules, which would not only hamper competition and smooth functioning of the internal market, but also the ability of Member States to deal with borderless cybersecurity risks.

[1] The EU's Cybersecurity Strategy for the Digital Decade, JOIN (2020) 18 final.
[2] The EU's Cybersecurity Strategy for the Digital Decade, JOIN (2020) 18 final, Page 5.
[3] The EU's Cybersecurity Strategy for the Digital Decade, JOIN (2020) 18 final, Page 9.
[4] Proposal for a Regulation of the European Parliament and of the Council on Horizontal Cybersecurity requirements for Products with Digital Elements and amending Regulation (EU) 2019/1020, COM/2022/454 final, available at <EUR-Lex - 52022PC0454 - EN - EUR-Lex (europa.eu)>.
[5] Section 1, Explanatory Memorandum for the Proposed Cyber Resilience Act, COM(2022) 454 final, Page 1.
[6] Section 1, Explanatory Memorandum for the Proposed Cyber Resilience Act, COM(2022) 454 final, Page 1.
[7] Section 1, Explanatory Memorandum for the Proposed Cyber Resilience Act, COM(2022) 454 final, Page 1.
[8] Major instruments include the NIS 2 Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) N0 910/2014 and Directive (EU) 2018/1972 and repealing Directive (EU) 2016/1148, the Cybersecurity Act – Regulation (EU) 2019/881 on ENISA and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013, and several pieces of sectoral legislation, including the Radio Equipment Directive (Directive 2014/53/EU) and the Medical Devices Regulation (Regulation (EU) 2017/745) among others.
[9] Section 1, Explanatory Memorandum for the Proposed Cyber Resilience Act, COM(2022) 454 final, Page 2.

2 A Closer Look at the Proposal

This partial regulatory vacuum led to the European Commission putting forward the proposal for the Cyber Resilience Act (CRA) in September 2022.[10] The proposed Regulation lays down horizontal cybersecurity requirements for all products with digital elements. In brief, the proposed Regulation lays down:

a) rules for placing products with digital elements on the market to ensure the cybersecurity of such products;
b) essential requirements for the design, development and production of products with digital elements;
c) essential requirements for the vulnerability handling processes put in place by manufacturers to ensure the cybersecurity of products with digital elements during the whole life cycle;
d) rules on market surveillance and enforcement.[11]

2.1 What does the CRA proposal cover?

The proposed Cyber Resilience Act will apply to all 'products with digital elements whose intended or reasonably foreseeable use includes a direct or indirect logical or physical data connection to a device or network'.[12] Accordingly, those products with digital elements that have no link to another device or to the internet are out of the scope of the proposed CRA. The proposal further defines 'products with digital elements' in a broad manner to mean 'any software or hardware product and its remote data processing solutions including software or hardware components to be placed on the market separately'.[13] Thus, the proposed CRA will also apply to software as a separate product from hardware.[14]

In general, Software-as-a-Service (SaaS) is excluded from the scope of the proposed CRA, except if it relates to (i.e., they are designed and developed for) a product with digital elements which cannot perform one of its functions without it.[15] In those cases, SaaS may fall within the scope of the proposed CRA.[16] Furthermore, free and open-source software are excluded from the scope of the proposed CRA.[17] Finally, the proposed CRA will not prevent presenting and using a product with digital elements that does not comply with the proposed CRA at trade fairs, exhibitions and demonstrations[18] nor will it prevent making unfinished software which does not comply with the proposed CRA available for testing purposes.[19] Overall, the scope of the proposed Regulation extends beyond IoT devices as it also includes, for instance, software applications, routers, and password managers.[20]

[10] Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1010, COM(2022) 454 final (hereafter CRA proposal).
[11] Article 1 CRA proposal.
[12] Article 2(1) CRA proposal.
[13] Article 3(1) CRA proposal.
[14] Pier Giorgio Chiara, 'The Cyber Resilience Act: The EU Commission's Proposal for a Horizontal Regulation on Cybersecurity for Products with Digital Elements' (2022) 3 International Cybersecurity Law Review, 258.
[15] Recital 9 of the CRA proposal states that the proposed CRA '(...) does not regulate services, such as Software-as-a-Service (SaaS), except for remote data processing solutions relating to a product with digital elements understood as any data processing at a distance 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 on of its functions (...)'.
[16] Chiara (n14) 259.
[17] Recital 10 CRA proposal.
[18] Article 4(2) CRA proposal.
[19] Article 4(3) CRA proposal.
[20] Article 2(2) and 2(3) of the CRA proposal clarifies that the proposed CRA will not apply when there is *lex specialis*. More specifically, the proposed CRA will not apply to products with digital elements which already fall within the scope of Regulation 2017/745 (Medical Devices Regulation), and Regulation (EU) 2017/746 (Regulation on in vitro diagnostic medical devices), and Regulation (EU) 2019/2144 (Automotive type-approval general regulation) or to products with digital elements that have been certified in accordance with Regulation (EU) 2018/1139 (Common rules in civil aviation). Furthermore, as stated in Article 2(5) of the proposed CRA, those products with digital elements exclusively developed for national security, military purposes or specifically designed to process classified information are also excluded from the scope of the proposed CRA.

2.2 Essential cybersecurity and vulnerability handling requirements

The CRA proposal lays down a baseline of essential cybersecurity requirements and vulnerability handling requirements for all products with digital elements. Products with digital elements can only be made available on the market provided that 1) the essential cybersecurity requirements have been met under the condition that they are properly installed, maintained, used for their intended purpose or under conditions which can reasonably be foreseen, and, where applicable, updated; and 2) the processes put in place by the manufacturer comply with the essential vulnerability handling requirements.[21]

The essential cybersecurity requirements entail that products with digital elements are designed, deployed, and produced in such a way that they ensure an appropriate level of cybersecurity based on the risk envisioned, on the one hand, and are delivered without any know exploitable vulnerabilities, on the other hand.[22] Furthermore, where applicable and on the basis of the risk assessment carried out, products with digital elements are required to abide by a set of more specific requirements, such as, for instance, being delivered with a 'secure by default' configuration, having appropriate access control mechanisms, protecting the confidentiality and integrity of the data processed, personal or otherwise, and the availability of essential functions.[23]

Additionally, manufacturers must adhere to certain 'vulnerability handling requirements'.[24] These vulnerability handling requirements obligate manufacturers, for example, to identify, document, and remediate vulnerabilities, to regularly test the security of their products, to publicly disclose information about fixed vulnerabilities once a security update has been made available, to put in place a policy on coordinated vulnerability disclosure, and to take measures to facilitate the sharing of information about potential vulnerabilities.[25]

2.3 Obligations of economic operators

A wide array of stakeholders will have to adhere to the rules laid down in the CRA proposal. The proposed Regulation sets out obligations for economic operators across the entire value chain of products with digital elements, starting from obligations of manufacturers, up to obligations of distributors and importers.[26]

In order to place a product with digital elements on the market, manufacturers must ensure that it has been designed, developed and produced in accordance with the essential cybersecurity requirements.[27] Furthermore, manufacturers must ensure that vulnerabilities are handled effectively and in accordance with the vulnerability handling requirements.[28] Before market placement, the manufacturer must perform a conformity assessment of the product with digital elements and of the vulnerability handling processes it has put in place to demonstrate conformity.[29]

Pursuant to the risk-based approach of the proposed Regulation, manufacturers must also undertake an assessment of the cybersecurity risks, the outcome of which must be considered during the planning, design, development, production, delivery, and maintenance phases of the product with digital elements.[30] This

[21] Article 5 CRA proposal.
[22] Annex I, Section 1 CRA proposal.
[23] For a complete overview of the essential cybersecurity requirements see Annex I, Section 1 of the CRA proposal.
[24] Annex I, Section 2 of the CRA proposal.
[25] For a complete overview of the vulnerability handling requirements see Annex I, Section 2 of the CRA proposal.
[26] Articles 10-17 CRA proposal.
[27] Article 10(1) CRA proposal.
[28] Article 10(6) CRA proposal.
[29] Article 10(7) CRA proposal.
[30] Article 10(2) CRA proposal.

cybersecurity risk assessment needs to be included in the technical documentation[31] and be continuously updated.[32]

The manufacturer also has various documentation obligations. Before market placement, manufacturers must draw up technical documentation.[33] Once compliance with the essential cybersecurity requirements and vulnerability handling requirements has been demonstrated by the conformity assessment procedure, the manufacturer will draw up the EU declaration of conformity and affix the CE marking.[34] Manufacturers must also ensure that products with digital elements are accompanied with the information and instructions set out in Annex II, either in electronic or physical form, in a clear, understandable, intelligible and legible language.[35]

When it comes to cooperation with market surveillance authorities, manufacturers will, upon request, provide the market surveillance authority with all the information and documentation necessary to demonstrate conformity, and cooperate on any measures taken to eliminate the cybersecurity risks posed by the product with digital elements.[36] Manufacturers will keep the technical documentation and EU declaration of conformity at the disposal of market surveillance authorities for 10 years after market placement.[37] Furthermore, manufacturers will inform the authority about the cessation of its operations with the consequence of not being able to comply with the obligations laid down in the proposed Regulation.

The proposed CRA also lays down various reporting obligations for manufacturers. The manufacturer is required to notify ENISA (European Union Agency for Cybersecurity) of any actively exploited vulnerability contained in the product with digital elements, including details concerning that vulnerability and any mitigating measures taken, without undue delay and in any event within 24 hours of becoming aware of it.[38] In the event of a security incident occurring to the product with digital elements, the manufacturer must notify both ENISA, without undue delay,[39] and the user of the product including, where necessary, the corrective measures to be deployed to mitigate the impact of the incident.[40] Upon identifying a vulnerability in a component integrated in a product with digital elements, including in an open-source component, the manufacturer will report the vulnerability to the person or entity maintaining the component.[41]

Importantly, the importer or the distributor will be considered a manufacturer for the purposes of the proposed Regulation and will be subject to the obligations of manufacturers[42] if the importer or distributor places a product with digital elements on the market under his or her name or trademark or carries out a substantial modification of the product with digital elements already placed on the market.[43] A natural or legal person that carries out a substantial modification will also be considered a manufacturer and subject to the corresponding obligations.[44]

The proposed Regulation also lays down obligations for entities other than manufacturers, such as authorised representatives, importers, and distributors.[45]

2.4 Non-critical, critical, and highly critical products with digital elements

The proposed CRA adopts a risk-based approach whereby products with digital elements are divided in different categories (non-critical, critical, and highly critical), depending on the level of cybersecurity risk, and undergo

[31] Article 10(3) CRA proposal.
[32] Article 10(5) CRA proposal.
[33] Article 10(7) CRA proposal. For further details regarding the technical documentation see Article 23 and Annex V CRA proposal.
[34] Article 10(7) CRA proposal.
[35] Article 10(10) CRA proposal.
[36] Article 10(13) CRA proposal.
[37] Article 10(8) CRA proposal.
[38] Article 11(1) CRA proposal.
[39] Article 11(2) CRA proposal.
[40] Article 11(4) CRA proposal.
[41] Article 11(7) CRA proposal.
[42] Laid down in Article 10 and Article 11(1), (2), (4), and (7).
[43] Article 15 CRA proposal.
[44] Article 16 CRA proposal.
[45] For a complete overview see Article 12, 13 and 14 CRA proposal.

different conformity assessment procedures based on these different categories.[46] Critical products with digital element are further subdivided in Class I and Class II products. Class I products include, for instance, identity management software and network traffic monitoring systems. Class II products include, for instance, intrusion detection and/or prevention systems intended for industrial use, routers, and smart meters.[47] Critical products will be subject to specific conformity assessment procedures.[48] Furthermore, the European Commission will be allowed, through the adoption of delegated acts, to specify categories of highly critical products with digital elements for which the manufacturers shall be required to obtain a European cybersecurity certificate under a European cybersecurity certification scheme to demonstrate conformity with the essential requirements set out in Annex 1 or parts thereof.[49]

2.5 Conformity assessment procedures

The manufacturer will have to perform a conformity assessment of the product with digital elements by following one of the procedures set out in the proposed Regulation, including: 1) the internal control procedure; 2) the EU-type examination procedure followed by conformity to EU-type based on internal production control; 3) conformity assessment based on full quality assurance.[50] When Class I or Class II critical products are involved, the manufacturer will not be able to rely on the internal control procedure to show compliance.[51] With specific regard to Class I critical products, the conformity assessment procedures will 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 these do not exist.[52]

The manufacturer shall draw up the EU declaration of conformity which shall contain the elements specified in the relevant conformity assessment procedures and shall be continuously updated.[53] Before the placing on the market, the CE marking shall be affixed visibly, legibly, and indelibly to the product.[54]

2.6 The role of harmonised standards and certification schemes

The CRA proposal only lays down high-level essential requirements that products with digital elements will have to meet to be placed on the European market. These high-level requirements will later be detailed by harmonised technical standards drafted by European Standardisation Organisations.[55] Products in conformity with harmonised standards, or parts thereof, shall be presumed to be in conformity with the essential requirements of the proposed CRA.[56] Where harmonised standards are non-existent, insufficient, or unduly delayed, the European Commission may adopt common specifications.[57] The presumption of conformity shall extend to such common specifications. In addition, products with digital elements for which an EU statement of conformity or certificate has been issued under a European cybersecurity certification scheme adopted as per the Cybersecurity Act, and for which the European Commission specifies via implementing Acts that such certification scheme(s)

[46] Chiara (n 14) 259.
[47] For a complete overview of Class 1 and Class 2 critical products with digital elements see: Annex III of the CRA proposal.
[48] Article 24(2) and 24(3) CRA proposal.
[49] Article 6(5) CRA proposal.
[50] Article 24(1) CRA proposal, for more details see Annex VI CRA proposal.
[51] Article 24(2) and 24(3) CRA proposal.
[52] Article 24(2) CRA proposal.
[53] Article 20 CRA and Annex IV.
[54] Article 22 CRA proposal.
[55] Chiara (n 14) 263.
[56] Article 18(1) CRA proposal.
[57] Article 19 CRA proposal.

can provide a presumption of conformity for the CRA, shall also be presumed to be in conformity with the CRA's essential requirements, or parts thereof.[58]

This is in line with the approach towards market regulation taken by the New Legislative Framework, [59] strengthening the conditions regarding product safety for introducing products into the European market while also ensuring relevance and applicability for a broad range of products[60] The CRA also provides for contingencies wherein harmonised requirements do not exist, allowing the Commission to adopt common specifications in case standards have not been developed/adopted.[61]

2.7 Market surveillance, enforcement, and penalties

National market surveillance authorities will carry out market surveillance activities. In order to ensure effective enforcement, market surveillance authorities may impose administrative fines. [62] Non-compliance with the essential cybersecurity requirements and the obligations and reporting obligations of manufacturers shall be subject to administrative fines of up to €15 million or, if the offender is an undertaking, up to 2,5% of the total worldwide annual turnover.[63] Non-compliance with any other obligations shall be subject to administrative fines of up to €10 million or, if the offender is an undertaking, up to 2% of the total worldwide annual turnover.[64] An administrative fine of €5 million or, if the offender is an undertaking, up to 1% of the total worldwide annual turnover may be imposed for the supplying of incorrect, incomplete or misleading information to notified bodies and market surveillance authorities.[65]

[58] Article 18(3) CRA proposal.
[59] New Legislative Framework, available at < New legislative framework (europa.eu)>; Chiara (n 14) 262.
[60] Article 18(1) and 18(3) CRA proposal.
[61] Chiara (n14) 263.
[62] Article 53 CRA proposal.
[63] Article 53(3) CRA proposal.
[64] Article 53(4) CRA proposal.
[65] Article 53(5) CRA proposal.

3 What comes ahead?

Once finalised, the Cyber Resilience Act will contain the first horizontal key cybersecurity requirements for all products with digital elements, including IoT devices. These requirements harmonise than the current fragmented cybersecurity requirements for IoT devices and, crucially, also include vulnerability handling requirements. Currently the proposal has been provisionally assigned to the Committee on Industry, Research and Energy (ITRE), with the European Economic and Social Committee adopting their opinion on the proposal in December 2022.[66] It is still pending trilogue and subsequent adoption,[67] which might take a significant amount of time still.

From a global market perspective, once the proposal is adopted, non-compliant devices or components would be disallowed from entering the internal market. Manufactures based outside the EU would also be targeted, thereby raising the possibility of the CRA becoming an international reference point for IoT Cybersecurity, similar to the GDPR in terms of data protection.[68]

There is also bound to be interplay with other Union policies and legislation such as the NIS2 Directive,[69] which is one of several legislations the proposal defers to for sectoral application. This is important from the INTERSECT perspective: horizontal legislation covering IoT as a whole will significantly reduce the fragmentation caused by diverging vertical legislations, while also acting as a 'safety net' of sorts at the Union level for products that are not covered by sectoral regulation currently, while specific standards are developed for them.

[66] Legislative Train Schedule, Horizontal cybersecurity requirements for products with digital elements, available at , <Carriages preview | Legislative Train Schedule (europa.eu)>.
[67] European Parliament, EU Cyber-Resilience Act Briefing, EU Legislation in Progress [December 2022], Page 1, available at <EU cyber-resilience act (europa.eu)>.
[68] European Parliament, EU Cyber-Resilience Act Briefing, EU Legislation in Progress [December 2022], Page 6, available at <EU cyber-resilience act (europa.eu)>.
[69] Directive (EU) 2022/2555 of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).