BRIEFING
EU Legislation in Progress

European Parliament

EU cyber-resilience act

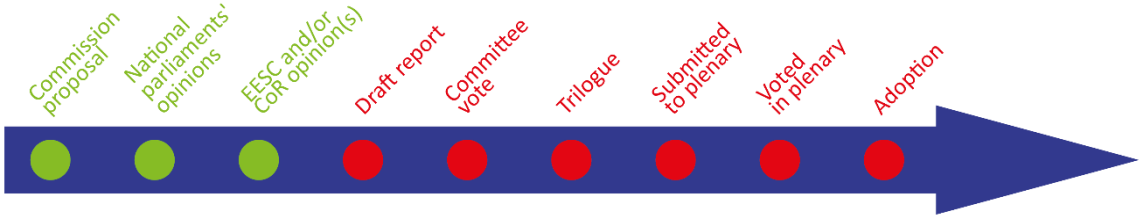
OVERVIEW

New technologies come with new risks, and the impact of cyber-attacks through digital products has increased dramatically in recent years. Increasingly, consumers have fallen victim to security flaws linked to digital products such as baby monitors, robo-vacuum cleaners, Wi-Fi routers and alarm systems. For businesses, the importance of ensuring that digital products in the supply chain are secure has become pivotal, considering three in five vendors have already lost money owing to product security gaps.

The European Commission's proposal for a regulation, the 'cyber-resilience act' therefore aims to impose cybersecurity obligations on all products with digital elements whose intended and foreseeable use includes direct or indirect data connection to a device or network. The proposal introduces cybersecurity by design and by default principles and imposes a duty of care for the life cycle of products.

In Parliament, the file has been provisionally assigned to the Committee on Industry, Research and Energy (ITRE).

Horizontal cybersecurity requirements for products with digital elements		
Committee responsible:	Committee on Industry, Research and Energy (ITRE)	COM(2022)454 15.9.2022
Rapporteur:	Nicola Danti (Renew, Italy)	2022/0272/COD
Shadow rapporteurs:	Henna Virkunen (EPP, Finland) Beatrice Covassi (S&D, Italy) Ignazio Corrao (Greens/EFA, Italy) Evžen Tošenovský (ECR, Czechia)	Ordinary legislative procedure (COD) (Parliament and Council on equal footing – formerly 'co-decision')
Next steps expected:	Publication of draft report	



EPRS | European Parliamentary Research Service

Authors: Polona Car and Stefano De Luca
Members' Research Service
PE 739.259 – December 2022

EN

Introduction

According to one industry forecast, the total number of internet of things (IoT) connected devices worldwide is set to more than double from 14.6 billion in 2022 to 30.2 billion by 2030. Another report estimates that the number of devices connected to IP networks will be more than three times the global population by 2023.

Cybersecurity flaws in connected products come with a cost. In its 2020 report Cybersecurity – Our Digital Anchor, the Commission highlighted how ransomware attacks hit organisations every 11 seconds around the globe. It is expected that by 2031 there will be a new attack on a consumer or business every 2 seconds, costing victims around US$265 billion (€251 billion) annually. Cybersecurity Ventures predicts that the general cost of cybercrime (e.g. ransomware, malware, cryptocrime) will reach US$8 trillion (€7.6 trillion) worldwide in 2023. The latest ENISA report on threat landscape in the EU revealed that 10 terabytes of data are stolen every month. Ransomwares scored the highest on the list of cyberattacks in the EU, followed closely by distributed denial of service attacks (DDoS), with the largest ever DDoS attack in Europe recorded in July 2022.[1] ENISA's report further reveals that all sectors are under threat, with public administration, online service providers and the general public being the most exposed to cyberthreats.

Given the growth in smart and connected products, a cybersecurity incident in one product can impact the entire supply chain, potentially disrupting social and economic activities across the internal market. A famous example of significant societal and economic costs relating to lack of cybersecurity is the WannaCry ransomware attack. This malware was designed to deny access to files on computers through encryption and demand a ransom payment for the decryption key. The WannaCry ransomware worm, launched in May 2017, affected computers worldwide by exploiting a Windows vulnerability. The UK National Health Service was heavily hit by WannaCry, which caused some hospital emergency departments to close. Another example is the Kaseya VSA supply chain attack of July 2021. This ransomware attacked over 1 000 companies and forced a supermarket chain to close all its 500 shops across Sweden.

In addition, European consumers' growing adoption of connected devices (e.g. smart-home appliances) and the related risks should not be underestimated. According to a 2021 Eurobarometer survey, 56 % of citizens believe that there is an increasing risk of falling victim to cybercrime, such as the theft or abuse of personal data, malicious software or phishing. For example, the German regulator banned Cayla in February 2017. Cayla was a connected doll conversing with children by sending microphone inputs to an app on a smartphone (iOS or Android device) via Bluetooth. The regulator considered the Cayla doll insecure both from a privacy point of view and as a potential concealed surveillance device. This because, due to security flaws, the doll could potentially allow anyone in close proximity to listen to and record conversations between the child and the toy – or other nearby conversations – by hacking the Bluetooth device connection.

Existing situation

In her 2021 State of the Union address, Ursula von der Leyen, the European Commission President, announced the cyber-resilience act proposal (CRA) stating that 'If everything is connected, everything can be hacked. Given that resources are scarce, we have to bundle our forces...This is why we need a European cyber defence policy, including legislation setting common standards under a new European cyber resilience act'.

Cybersecurity is one of the Commission's top priorities for a digital and connected Europe. The CRA is one of the building blocks of the Commission's EU cybersecurity strategy for the digital decade. It is also in line with the EU's priorities to create a Europe fit for the digital age in which digital transformation will benefit both people and businesses. The cybersecurity strategy acknowledges that improving cybersecurity is essential to both benefit from innovation, connectivity and automation and safeguard fundamental rights and freedoms (e.g. protection of personal data and

the freedom of expression). The existing EU cybersecurity framework comprises several pieces of legislation that cover specific aspects of cybersecurity from different angles.

Dealing with criminal law, the Directive on Attacks against Information Systems came into force in 2013 and harmonised criminalisation and penalties for a number of offences directed against information systems. Moving to critical infrastructure, the Directive on Security of Network and Information Systems across the EU (the NIS Directive) entered into force in 2016, bringing horizontal legal measures to boost the overall level of cybersecurity in the EU, with a focus on protecting critical infrastructure. The NIS Directive is now to be replaced by the recently adopted Directive on the Security of Network and Information Systems (NIS2), which tackles its predecessor's limitations. In addition, sectoral legislation, such as the Directive on the Resilience of Critical Entities (CER) and the Regulation on Operational Resilience of the Financial Sector (DORA) set specific security and reporting requirements in their fields. As far as information and communication technology (ICT) products, services and processes are concerned, in 2019 the EU Cybersecurity Act strengthened the powers of the European Union Agency for Cybersecurity (ENISA) and introduced a **voluntary certification scheme** to apply to the cybersecurity features of an ICT product, service or process. Although the scheme remains voluntary for businesses, it may be used for compliance with the mandatory safety requirements of other legal acts.

In addition, the EU has adopted specific sectoral legislation on safety for products with digital elements in the Radio Equipment Directive (RED), the Medical Device Regulation, the In Vitro Diagnostic Medical Devices Regulation, the Vehicle General Safety Regulation, in the Common Rules in Civil Aviation Regulation and in the proposed machinery regulation. Lastly, the proposed artificial intelligence act mandates an ex-ante conformity assessment for high-risk AI systems.[2] At present, there are no general cybersecurity requirements at EU level for all hardware and software that are not specific to certain products or sectors. Indeed, Thierry Breton – Commissioner for the Internal Market – has said that 'most of the hardware and software products are currently not covered by any legislation regarding their cybersecurity'. The opinion of the ENISA advisory group confirms this picture, reporting that 'connected devices for consumers often do not include the most basic security features, and are therefore vulnerable to the most basic cyberattacks and misuse'. For instance, the delegated regulation supplementing the RED Directive deals with the security of consumer IoT devices by imposing a high level of requirements on manufacturers of internet-connected wireless and wearable radio equipment (i.e. requiring them to incorporate safeguards to ensure personal data protection). However, because of a 30-month transition period, the RED requirements will be applicable only from August 2024. Once the proposed CRA becomes applicable, the RED delegated regulation will then be repealed. In addition, the EU legal framework does not address the cybersecurity of non-embedded software represented by applications such as navigation software or in-car entertainment systems. Moreover, economic operators' response to the vulnerabilities of products with digital elements throughout their lifecycle is an issue that demands further attention.

The absence of a cybersecurity legal framework for products with digital elements incentivises the development of potentially diverging national rules among Member States, threatening an open and competitive single market. In this regard, EU countries have already adopted or proposed cybersecurity requirements for consumer IoT. For example, Finland and Germany have applied certain security measures on a voluntary basis. Countries outside the EU are also busy addressing this issue. For example, Brazil, China and Japan have adopted mandatory certification schemes for certain digital products. In the UK, a proposed bill would introduce mandatory security requirements and require a statement of compliance before a consumer IoT product can be placed on the market. In the US, an Executive Order on Improving the Nation's Cybersecurity has been published, identifying software bills of materials (SBOMs) as a crucial tool to improve the security and integrity of the software supply chain.[3]

Parliament's starting position

In its resolution of 3 October 2017, Parliament stressed that particular attention should be paid to the security of IoT devices, calling for a security by design approach to be taken to all such devices. Parliament encouraged the private sector to take voluntary measures to support trust in the security of software and hardware.

In similar vein, in its 10 June 2021 resolution, the Parliament called for security by design and cyber-resilience for all internet connected products along the entire supply chain. More specifically, Parliament welcomed the 'Commission's plans to propose horizontal legislation on cybersecurity requirements for connected products and associated services', with a view to harmonising national laws and hence preventing fragmentation of the single market. In addition, it asked the Commission to shape a horizontal regulation on cybersecurity requirements for apps, software (including embedded software), and operating systems by 2023. This regulation should mandate manufacturers to include information for users on the duration of security updates.

Council starting position

In its conclusions of 2 December 2020, the Council acknowledged the increased cybersecurity risks for connected devices. Furthermore, it expressed the need to minimise cybersecurity risks to protect consumers as well as to increase Europe's cyber-resilience to foster competitiveness and innovation. The Council stated that 'cybersecurity and privacy should be acknowledged as essential requirements in product innovation, the production and development processes – including the design phase (security by design) – and should be ensured throughout a product's life cycle and across its supply chain'.

In its conclusions of 23 May 2022 the Council called upon the Commission to propose common EU cybersecurity requirements for connected devices and associated processes and services by the end of 2022 through the CRA. According to the Council, the proposal should take into account 'the need for a horizontal and holistic approach that covers the whole lifecycle of digital products, as well as existing regulation, especially in the area of cybersecurity'.

Preparation of the proposal

The European Commission commissioned a study to support the preparation of the impact assessment (IA) that was published together with the proposal. In addition, to collect stakeholders' opinions, the Commission organised: an open public consultation (OPC), workshops, surveys and expert interviews. Special efforts were also made to gather views from SMEs on the impacts of possible policy options.

Study on cybersecurity requirements for ICT products

The study on the need for cybersecurity requirements for ICT products was published in December 2021. It aimed to analyse the regulatory landscape for ICT products and come up with possible policy options. The study's gap analysis compared the cybersecurity objectives of certification schemes set out in the cybersecurity act against cybersecurity requirements of 37 identified EU legal acts relating to products with digital elements. It concluded that the current EU legislative framework does not cover cybersecurity sufficiently. To support the IA further, a second exploratory study (see Annex 8 of the IA) was commissioned at the beginning of 2022 to underpin all possible policy solutions with a solid and coherent analysis.

Open public consultation and call for evidence

The open public consultation (OPC) ran from 16 March to 25 May 2022 and gathered replies from 167 respondents, including representatives of the ICT industry, national authorities, consumer

associations, conformity assessment bodies, academics and the general public. More than half of the replies came from Belgium and Germany, and only 22 from non-EU countries. The OPC sought stakeholders' views on current and emerging problems relating to the cybersecurity of products with digital elements, which includes a very broad range of devices directly or indirectly connected to another device or to the network. The overall majority of respondents regarded horizontal requirements for hardware and software to be the most effective measure. Furthermore, 79 % of respondents supported the CRA's third-party conformity assessment procedure for digital products under certain circumstances (e.g. for high-risk products). For 88 % of respondents, hardware and software manufacturers should be responsible for the full life cycle of products with digital elements (e.g. providing updates).

As part of the preparation of the proposal, the Commission organised a call for evidence for an impact assessment (from 16 March to 25 May 2022), where interested stakeholders could provide feedback on the Commission's understanding of the problem and possible solutions. In addition, stakeholders provided their views on the expected impacts of the various options tabled in the CRA proposal. A total of 109 stakeholders responded to this call. The general opinion was that regulatory intervention is required, as the status quo is not an option in the fast evolving market, and that security risks that are part of this evolution need to be addressed. An additional feedback period was opened until 17 December 2022.

Impact assessment

The Commission conducted an IA for the current proposal to address the problem of the low level of cybersecurity of products with digital elements marketed in the Union; and poor user awareness as regards product cybersecurity. The IA analysed four policy options for EU action regarding cybersecurity requirements for products with digital elements. The four options included: i) soft law approach and voluntary measures; ii) sectoral regulatory intervention, not addressing non-embedded software; iii) a mixed approach, making a distinction between tangible products (horizontal rules) and non-embedded software (soft-law approach); and iv) a horizontal regulatory intervention introducing cybersecurity requirements for a broad scope of products with digital elements, including non-embedded software.

Option 4 prevailed as the preferred one, as it could provide legal certainty for companies and a coherent European approach to the cybersecurity of products with digital elements, preventing fragmentation of the digital internal market. According to the IA's estimation, option 4 b), including all software and third-party assessment could reduce the number of cybersecurity incidents by approximately 20 to 33 %. It was estimated that this option would result in companies incurring €29 billion total in compliance costs. However, the costs would be largely offset by the EU-wide reduction of costs relating to cybersecurity incidents, estimated at between €180 billion and €290 billion annually. Non-quantifiable benefits should be added, such as i) increased uptake of products with digital elements because of the increased trust in technology or ii) a decrease in risk mitigation costs for users, to name just two.

The IA was submitted to the Regulatory Scrutiny Board (RSB) on 13 May 2022 and received a positive opinion with reservations on 8 July 2022. The RSB required that the scope of the initiative be placed in the wider context of recent EU initiatives on cybersecurity, explaining why existing measures do not address the issue sufficiently. The RSB noted that concrete evidence of the risk of market fragmentation through uncoordinated national initiatives was missing. The RSB observed that the cost-benefit analysis was incomplete as it did not explain sufficiently the underlying methodology and figures attributed to the different options, which are also not adequately compared. The RSB further observed that types and views of different stakeholders were not presented in a satisfactory manner.

EPRS published an initial appraisal of the Commission impact assessment of the cyber-resilience act in December 2022.

The changes the proposal would bring

As the first ever EU-wide legislation of its kind, the Commission proposed the EU cyber-resilience act in order to bolster the cybersecurity of products with digital elements (digital products) in the European Union and to address existing regulatory cybersecurity gaps. Indeed, devices with digital elements that do not comply with the requirements introduced by the proposed regulation would be banned from the European market. As the proposed CRA would also target digital products from non-EU vendors when marketed in the EU, it might have the potential to impact cybersecurity standards for such products beyond EU borders. The EU would become the international point of reference on cybersecurity of connected devices in the way that the General Data Protection Regulation did for privacy. Indeed, non-EU companies might find it more convenient to apply the proposed CRA rules – mandatory to access the EU single market with their digital products – as a default framework for their global operations than to create different products or processes for different markets.

Principle and objectives

The proposed CRA is a **piece of horizontal legislation** based on Article 114 of the Treaty on the Functioning of the EU (ordinary legislative procedure applies) dealing with legislative harmonisation and the establishment and functioning of the internal market. It aims to harmonise cybersecurity rules for the placing on the market of products with digital elements. EU standards based on the CRA would raise the level of cybersecurity for digital products in the European Union, benefiting both businesses and consumers.

The proposed CRA has two main objectives for digital products (e.g. hardware and software) and its aim is to create the conditions for the development of secure digital products by ensuring that hardware and software products are placed on the market with fewer vulnerabilities. It also aims to oblige manufacturers to take security seriously throughout products' life cycles, and to equip users to take cybersecurity into account when selecting and using products.

Scope

In its article 3(1), the CRA defines **products with digital elements** as 'any software or hardware product and its remote data processing solutions, including software or hardware components to be placed on the market separately'. In article 2(1), it further clarifies that the proposed regulation applies to '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'. Therefore, the proposed CRA is a horizontal regulation that, with few exceptions, covers a very wide range of digital products, such as connected devices (e.g. consumer and industrial IoT), operating systems and non-embedded software. The proposal also covers artificial intelligence (AI) systems, including the cybersecurity of products with digital elements that are classified as high-risk AI systems.

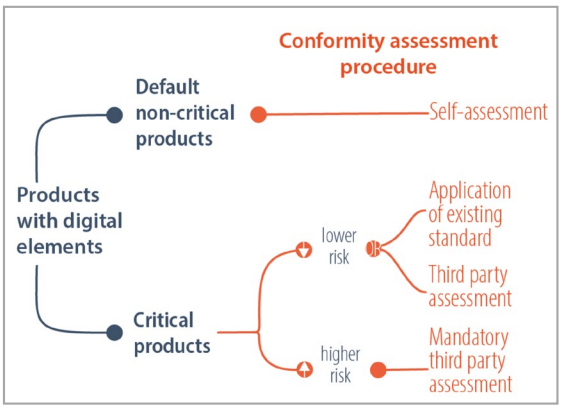
Products excluded from the proposal's coverage are: digital devices covered by specific sectoral regulations,[4] software-as-a-service (SaaS) such as clouds, unless they are part of integral remote data processing solutions for a product with digital elements. Last but not least, in order not to hamper innovation or research, free not-for-profit open source software[5] is not covered by this proposal.

The proposed CRA divides digital products covered by the regulation into two main categories, based on their level of risk. The first is **default non-critical products** i.e. hardware and software with a low level of criticality (e.g. smart home assistants or connected toys). The second is **critical products**, which are further divided in two sub-categories, class I lower risk (e.g. routers) and class II higher risk (e.g. server operating systems, desktops, and mobile phones) reflecting criticality and intended use.

Based on their level of risk, the above-mentioned digital products would be subject to less or more stringent obligations ranging from a simple cybersecurity self-assessment to a third-party conformity assessment.

The proposed CRA places cybersecurity obligations on different economic operators as appropriate for their role and responsibilities in the supply chain. **Manufacturers** must ensure that digital products comply with essential cybersecurity requirements and conformity assessment procedures before placing them on the market. In addition, they need to record technical documentation and abide by notification obligations for cybersecurity breaches. **Importers** must place on the market only digital products that comply with essential cybersecurity requirements and bear the CE marking. **Distributors** must verify that the digital products bear the CE marking. They also have a duty of care to ensure that manufacturers and importers have complied with their obligations under the act.

Figure 1 – Cyber resilience conformity assessment



Source: European Commission.

Main provisions

Cybersecurity by design and by default

Manufacturers must consider cybersecurity from the design and development phase of the digital product by using secure-by-default configurations and avoiding known exploitable vulnerabilities. The annexes of the proposed CRA include i) the information manufacturers should make available to users; ii) conformity assessment procedures digital products must go through; and (iii) the technical documentation to provide. In addition, iv) Annex I(2) details the vulnerability handling requirements manufacturers must follow to assure the cybersecurity of digital products.

Essential cybersecurity and vulnerability handling requirements, including reporting obligations

The proposed CRA splits the cybersecurity obligations for manufacturers between i) security requirements relating to the properties of digital products and ii) vulnerability handling requirements.

Significant **cybersecurity requirements** listed in Annex I include obligations to i) design, develop and produce digital products in such a way that limits their attack surface and reduces the impact of any incident based on the risks; ii) deliver digital products without known exploitable vulnerabilities; iii) protect the confidentiality and integrity of data stored, transmitted or processed; (iv) process only data, personal or other, that are strictly necessary to the functioning of the digital product– 'data minimisation'.

As far as **vulnerability handling** is concerned, after the product has been placed on the market, manufacturers must deploy, for example, regular tests and reviews of their digital products' security, keep a record of vulnerabilities identified, and remediate them by providing free security updates and patches. The manufacturers will be required to do so for (i) the expected product lifetime or for (ii) a period of 5 years, whichever is shorter.

Finally, manufacturers will have to report actively exploited vulnerabilities and security incidents to the European Union Agency for Cybersecurity (ENISA) within 24 hours of becoming aware of them.

Conformity assessment and compliance

The conformity assessment procedure applied to demonstrate compliance with the requirements mentioned above differs based on the criticality of the digital product. For non-critical products, manufacturers will be responsible for declaring that their products satisfy the essential security

requirements of Annex I (self-assessment). For critical products, however, manufacturers must apply harmonised security standards (e.g. EU cybersecurity certification scheme) or provide a third-party conformity assessment by authorities to be designated by the Member States.

The digital products demonstrating compliance with the security requirements and the conformity assessment procedures will obtain an EU declaration of conformity valid in all EU Member States and bear the CE marking according to the general principles of Regulation (EC) 765/2008.

Fines

Member States will appoint market surveillance authorities, which will be responsible for the enforcement of the proposed CRA obligations.

In cases of non-compliance with the obligations set out in the proposal, the following maximum fines would apply based on the type of infringement and nature of the economic operator: **manufacturers** could risk a fine of €15 million or 2.5 % of their total annual turnover worldwide, whichever is higher, for non-compliance with the security requirements listed under Annex I. **Manufacturers**, **importers**, or **distributors** could risk a fine of €10 million or 2 % of their total annual turnover worldwide, whichever is higher for non-compliance with any other obligation laid down in the draft regulation.

Interplay between the conformity assessment procedure and existing or upcoming cybersecurity legislation

The proposed CRA and its conformity assessment dovetails with other pieces of existing or proposed legislation on cybersecurity. The proposal aims to harmonise the EU regulatory landscape by introducing cybersecurity requirements for products with digital elements, without overlapping with requirements stemming from the following pieces of legislation.

Starting with **existing legislation**, the CRA proposal would complement the baseline EU cybersecurity framework, namely the NIS2 Directive and the EU Cybersecurity Act. The NIS2 Directive puts in place cybersecurity requirements and incident reporting obligations for essential and important entities to increase their resilience, for example, a clear obligation to demonstrate how those entities have assessed the security level of the ICT products and services. Therefore, the enhanced and certified level of cybersecurity of products with digital elements – to be reached through the CRA – would facilitate compliance by the entities in the scope of the NIS2 Directive and would strengthen the security of the entire supply chain.

The EU Cybersecurity Act allows the development of voluntary certification schemes. Each scheme includes references to relevant standards, technical specifications and other cybersecurity requirements defined in the scheme. Digital products respecting such voluntary cybersecurity certification schemes would be presumed to be compliant with the conformity assessment of the proposed CRA. Finally, the proposed CRA applies to radio equipment within the scope of the RED delegated regulation. The proposal is aligned with the requirements of the RED delegated regulation imposing high-level standards on manufacturers of internet-connected wireless and wearable radio equipment. To avoid a regulatory overlap, the Commission would repeal the RED delegated regulation with respect to specific radio equipment that is also covered by the draft CRA regulation once it enters into force.

Moving to **legislative proposals** under adoption, the proposed CRA conformity assessment would take into consideration the provisions of the artificial intelligence act and the regulation on machinery products proposals. As a general rule, for devices also classified as high-risk AI systems, the conformity assessment procedure specified under the CRA proposal shall apply to demonstrate compliance with the proposed artificial intelligence act security requirements. However, exceptions apply for certain AI critical products. Digital products also covered in the proposed regulation on machinery products, and for which a conformity assessment has been required, would be

considered to be in conformity with the proposed CRA providing the health and safety requirements of the sectoral machinery regulation are met.

Advisory committees

The European Economic and Social Committee (EESC) is supportive of the process of harmonising cybersecurity rules at Member State level. However, it points out potential difficulties with the monitoring and oversight of the implementation of the CRA since the proposal covers virtually all digital products. The EESC underlines the need to clarify the material scope of the CRA and take care of the particular needs of SMEs when setting criteria for services provided by the certification authorities. In addition, the EESC points out that ENISA should be given sufficient resources given its enlarged responsibilities. The EESC suggests that the Commission should draft guidelines for manufacturers and consumers on the application of the CRA in practice. Finally, the EESC notes that appointing different certification authorities in the cybersecurity realms under different EU legal acts could increase the administrative burden already imposed on manufacturers operating on the market. The EESC adopted its opinion during its December 14-15 2022 plenary session.

National parliaments

The subsidiarity deadline for national parliament has been set at 19 December 2022. So far the Czech Chamber of Deputies and Irish houses of Oierachtas have issued opinions on the proposal.

Stakeholder views[6]

Scope of the proposal: What kind of software?

Inclusion of all software in the scope of the proposal would be premature according to DigitalEurope (representing digital technology industry in Europe) as cyber-resources are scarce both for the industry and for governments. On the other hand, Eurosmart (representing the European digital security industry), supports the inclusion of software as a product under the relative liability rules as this would help to acknowledge the cybersecurity value chain when products relying on software are placed on the market. Eurosmart advocates for encryption as a European way to ensure a high level of security in which privacy considerations are taken on board. Internet Society – a non-governmental organisation (NGO) promoting internet development – pleads for clear exclusion of not-for-profit open source licence software from the scope of the CRA, because of the unclear definition of commercial activity in the proposal. The role of distributors should also be refined to exclude platforms that distribute open source software. In its view, the certification procedure and fines that might apply could hinder development of open source software, which underpins the development of the internet. This could cause the withdrawal of open source products from the internal market, which could affect innovation in Europe.

Personal data as essential cybersecurity requirements

The European Data Protection Supervisor (EDPS) recommends considering personal data protection to be an 'essential cybersecurity requirement' of products with digital elements. This should be done by applying the principle of data protection by design and by default. The proposal should clearly state that it does not aim to affect the powers of data protection authorities. The EDSP also recommends clarifying that obtaining a cybersecurity certification label under the proposal does not automatically assure compliance with the GDPR.

Classification of products based on risk

APPLiA (representing the European home appliance industry) advocates a clear distinction between low and high-risk products and for the definition of clear standards for each of those product categories. The European Digital SME Alliance called for a risk-based approach, where different

product categories would follow different procedures (e.g. imposing minimum requirements and compliance checks for low-risk products). Euroconsumers (association of consumer organisations) believes that the omission of consumer IoT products (e.g. connected devices intended for children) from the category of critical products should be reconsidered. In the association's view, such products could be potentially harmful if hacked, and a third-party risk assessment, mandatory for class II higher-risk critical products, could play a role in detecting vulnerabilities in such products. TIC Council (representing the testing, inspection and certification industry) is similarly concerned about the nature of consumer IoT products that currently fall within the low-risk category despite having the ability to collect, store and share data.

VDMA (representing mechanical and plant engineering industry) and ZVEI (German electrical and electronic manufacturers' association) are concerned that classifying all core components for networked machines and systems as critical products could lead to red tape for manufacturers. According to both associations, many industrial components are only used for non-critical purposes. They therefore fear that this approach could cause delays in Europe in the deployment of digital products and their components. In this respect, they propose making a reference to the intended use of the product.

Conformity assessment procedure

BEUC (the European Consumer Organisation) argued in favour of independent third-party conformity assessments also for certain products representing higher risks to consumers (e.g. safe home systems). In a similar vein, TIC Council favours conformity assessment by bodies that are independent from the product developer. They are afraid that self-assessment of non-critical products by the companies that manufacture them – which represent 90 % of digital products placed on the market – will lead to a certain amount of unsafe and unsecure products for consumers. TÜV Verband (an association of technical inspection agencies) believes that the CRA should 'not only define cybersecurity requirements, but it must also stipulate effective instruments with which compliance with these requirements can be reliably verified'. The organisation considers that all critical products should undergo a compulsory assessment by independent assessment bodies. In contrast, CCIA (a computer and communications industry association) considers the new conformity assessment procedures for digital products excessive, with the potential to stop the development of new technologies and services.

Concerns were expressed over the absence of horizontal cybersecurity standardisation schemes. For example, VDMA worries that the absence of appropriate standards could cause delays in the delivery of approved products. Eurosmart encourages different standardisation initiatives to support certification schemes for different product types as described by the CRA. Eurosmart believes that cybersecurity for critical products with digital elements should be addressed under the EU cybersecurity act's 'high' level certification scheme. Satisfaction of this scheme should be considered to provide a presumption of conformity with the CRA requirements because it contains mandatory penetration testing to assess the resilience of critical products.

Duty of care and product lifecycle

Euroconsumers has reservations about the limited definition of the lifespan of a product where the duty of care duration is set to maximum 5 years. This could be problematic, for example for users of smart home security systems that are expected to last much longer than 5 years. Along these lines, BEUC asked for a requirement that manufacturers provide software updates for the whole life-cycle of a product. Contrary to this, the European Digital SME Alliance welcomed the limiting of the obligation to provide updates.

Notification fatigue

Blackberry stresses the burden on companies to report cybersecurity incidents to different authorities. Indeed, companies will have to report a single incident: i) to ENISA under the CRA for digital products;

ii) to the national competent authority under NIS2 as critical operators; iii) to a financial institution under DORA if software was used by a financial entity; and iv) to a national data protection authority if personal data is involved. Bitkom (a German digital industry association) also stresses the problem of extensive documentation obligations for companies, generating a high level of red tape.

Academic views

Need for horizontal regulation

One recent article[7] recognised the insufficiency of the existing EU legal framework to address the cybersecurity of digital products. It underlined that potential limits to the shared competences in this sector need to be examined, as cybersecurity is not an exclusive competence of the EU. In addition, it recommended applying the proposed regulation to the entire supply chain and supported the full transparency concept. This means that understanding the cryptography and cybersecurity tools of the product would not qualify as a trade secret for non-disclosure of information (except for certain exemptions such as hardware verification mechanisms). Similarly, one expert[8] advocates harmonised EU cybersecurity rules, as this would be the most efficient way to increase cyber-resilience by enhancing the trust of users and the prominence of products with the CE marking. According to the author, the CRA contributes to the evolution of the concept of cybersecurity and goes beyond technical IT security. A horizontal approach would help to ensure legal certainty by avoiding further overlapping of legislation and market fragmentation. The Center for Data Innovation, meanwhile, stated that the horizontal framework proposed by the CRA could entail high compliance costs and might not be future-proof enough. Therefore, they recommended an approach that recognises sectoral differences in cybersecurity needs by regulating each sector individually. This would minimise costs.

Continuous risk-assessment

According to the above-mentioned article by the Center for Data Innovation, the CRA should comprise the need for continuous security risk-management, but the cost should not fall necessarily upon the manufacturers. Digital products should be kept secure throughout their life cycles, with penetration testing being part of this maintenance system. The authors advocate for assessment by Member States' dedicated authorities rather than third-party conformity assessment, because in their view private organisations should not be assessing the security of digital products.

Surveillance and enforcement

The above-mentioned article also made several interesting proposals regarding surveillance and enforcement. The article outlined two possible approaches for the CRA: creation of common rules at EU level and enforcement of them at national level; or standardisation of some measures at European level though a central authority such as ENISA and entrusting the remaining ones to the national authorities. Both approaches will need to take into account voluntary certification schemes brought in by the cybersecurity act, which are still under development.

Finally, it recommended stringent enforcement mechanisms by giving national authorities inspection powers. As far as staff and sanctions are concerned, researchers suggested staffing requirements similar to those in AI act proposal and sanctions similar to those given in the GDPR, with the additional possibility to ban cyber insecure products from the market.

Legislative process

In the Parliament, the file has been assigned to the Committee on Industry, Research and Energy (ITRE) and Nicola Danti (Renew, Italy) has been appointed as rapporteur. The Committees on Internal Market and Consumer Protection (IMCO) and on Civil Liberties, Justice and Home Affairs (LIBE) have been asked for their opinions.

In the Council, a progress report was presented by the Czech Presidency to the Transport, Telecommunications and Energy Council meeting on 6 December.

EUROPEAN PARLIAMENT SUPPORTING ANALYSIS

The NIS2: A high common level of cybersecurity in the EU, EPRS, European Parliament, June 2022.

ENISA and a new cybersecurity act, EPRS, European Parliament, July 2019.

Artificial intelligence act, EPRS, European Parliament, January 2022.

Strengthening cyber resilience, Initial Appraisal of a European Commission Impact Assessment, EPRS, December 2022

OTHER SOURCES

Horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act), Legislative Observatory (OEIL), European Parliament.

Cybersecurity, our digital anchor, European Commission, Joint Research Centre, 2020.

ENDNOTES

1 The Cisco report estimates that DDoS attacks will double from 7.9 million in 2018 to 15.4 million by 2023.

2 According to Recital (27) the draft AIA, 'AI systems identified as high-risk should be limited to those that have a significant harmful impact on the health, safety and fundamental rights of persons in the Union and such limitation minimises any potential restriction to international trade, if any'.

3 Congressional Research Service report

4 Regulations on medical devices, in-vitro diagnostic medical devices, civil aviation safety, on-type approval requirements for motor vehicles and their trailers and systems. Furthermore, components and products developed exclusively for national security or military purposes and products specifically designed to process classified information are also excluded from the scope of the proposed CRA.

5 This is the case of software openly shared and freely accessible. Indeed, it is believed that open source software is paradoxically less exposed to cybersecurity risks. This is because when many programmers are involved in the continuous development of software, there is a higher chance that vulnerabilities are spotted by someone throughout the development or update process.

6 This section aims to provide a flavour of the debate and is not intended to be an exhaustive account of all different views on the proposal. Additional information can be found in related publications listed under 'European Parliament supporting analysis'.

7 See K. Ludvigsen and S. Nagaraja, The Opportunity to Regulate Cybersecurity in the EU (and the World): Recommendations for the Cybersecurity Resilience Act, Cornell University, May 2022.

8 See P.G. Chiara, 'The Cyber Resilience Act: the EU Commission's proposal for a horizontal regulation on cybersecurity for products with digital elements', *International Cybersecurity Law Review*, November 2022.

DISCLAIMER AND COPYRIGHT

eprs@ep.europa.eu (contact)

www.eprs.ep.parl.union.eu (intranet)

www.europarl.europa.eu/thinktank (internet)

http://epthinktank.eu (blog)

First edition. The 'EU Legislation in Progress' briefings are updated at key stages throughout the legislative procedure.