EuZ
ZEITSCHRIFT FÜR EUROPARECHT

AUSGABE:
02|2023

LEITARTIKEL 1:

Mira Burri / Zaira Zihlmann
The Cyber Resilience Act - An appraisal and contextualization

LEITARTIKEL 2:

Okan Yildiz / Rolf H. Weber
Market Definition and Market Power in the Era of Blockchain

The EU Cyber Resilience Act – An appraisal and contextualization

Mira Burri/Zaira Zihlmann*

Table of contents

A. Introduction B 2

B. Drivers of a horizontal cybersecurity regulation B 4
I. Creating an Internet of Secure Things through harmonization and mandatory requirements B 4
1. Protecting consumers by imposing mandatory requirements for all connected devices B 5
2. Ensuring a coherent cybersecurity framework via horizontal regulation B 7
II. Strengthening digital sovereignty via cybersecurity regulation B 8
1. EU's cybersecurity activities B 8
2. Digital sovereignty and EU's re-sovereignization B 11

C. The proposed Cyber Resilience Act: Analysis of selected key aspects B 13
I. Horizontal regulatory intervention with a broad scope of application B 15
1. Regulatory intervention based on Art. 114 TFEU B 15
2. Extensive material scope B 16
3. Complex interplay with other regulations B 20
4. Addressees along the supply chain B 22
5. CRA's territorial scope B 22
II. Risk-based classification of products B 25
III. Obligations of economic operators along the supply chain and throughout the life-cycle of products B 29
1. Extensive obligations of manufacturers B 29
2. Importers as watchdogs B 36
3. Few duties for distributors B 37

* Mira Burri is Professor of International Economic and Internet Law at the Faculty of Law of the University of Lucerne; Zaira Zihlmann is a doctoral fellow at the same institution. Authors thank Gaurav Sharma for his helpful comments. All URLs have been last accessed on 17 February 2023.

IV. Comprehensive market surveillance and enforcement mechanisms B 38
V. Significant administrative fines B 41

D. Concluding observations and outlook B 42

A. Introduction

The onset of a "fourth industrial revolution" was heralded a few years ago, a term coined to describe the advancing fusion of technologies that blurs the lines between the physical, digital, and biological realms.[1] Crucial part in this transformation is played by the Internet of Things (IoT)[2] as "a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies."[3] The number of devices connected to the IoT is huge and growing. There are currently more IoT devices than there are humans on the planet,[4] and it is estimated that by 2025 there will be 30.9 billion IoT devices worldwide, with 4.3 billion of those in the European Union (EU).[5] Yet, a large number of these connected devices come with a low level of cybersecurity.[6] This raises serious concerns as more unsecured products also mean an extended attack surface and heightened cybersecurity risks for their users.[7] This becomes even more problematic as connected products by means of interlinked systems of sensors and actuators interact seamlessly with the physical realm in which they operate. Thus, the

1 Schwab Klaus, The Fourth Industrial Revolution, Geneva 2016, 12.

2 Carr Madeline/Lesniewska Feja, Internet of Things, Cybersecurity and Governing Wicked Problems: Learning from Climate Change Governance, International Relations 2020, 392.

3 Definition according to the International Telecommunication Union. ITU, Recommendation Y.2060, Overview of the Internet of Things, 2012, <https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-Y.2060-201206-I!!PDF-E&type=items>.

4 Tasheva Iva/Kunkel Ilana, In a Hyperconnected World, Is the EU Cybersecurity Framework Connected?, European View 2022, 187.

5 Statista, Internet of Things (IoT) and Non-IoT Active Device Connections Worldwide from 2010 to 2025, September 2022, <https://www.statista.com/statistics/1101442/iot-number-of-connected-devices-worldwide/>.

6 Studies have shown that between 57% and 68% IoT devices have critical vulnerabilities. Roberts Paul F., Smart Toys Are Still Hackable (We Just Don't Talk about It), Forbes, 28 December 2022, <https://www.forbes.com/sites/paulfroberts/2022/12/28/smart-toys-are-still-hackable-we-just-dont-talk-about-it/>.

7 Cf. Johnson Shane D. et al., Crime and the Consumer Internet of Things, in: Gill Martin (ed.), The Handbook of Security, Cham 2022, 707.

security of these products is directly related to safety.[8] Moreover, given the strong cross-border nature of connected devices, an incident that initially affects a single entity or an EU Member State can often spread across organizations, industries and multiple Member States, and this within minutes.[9] To put it in the words of the European Commission's President Ursula von der Leyen: "[i]f everything is connected, everything can be hacked."[10] Following up on this expressed concern in her 2021 State of the Union address, she declared the EU's intention to take a leading role in cybersecurity and announced the project of a Cyber Resilience Act (CRA) – as a complement to EU's cybersecurity acquis with horizontal cybersecurity requirements for all products with digital elements[11] and the "first ever EU-wide legislation of its kind."[12] The CRA project advanced rapidly and was adopted by the Commission on 15 September 2022.[13]

If enacted, the CRA would allow, among other things, the banning of devices with digital elements that do not meet the requirements of the EU market. Given that the CRA may also apply to non-EU manufacturers' digital products once placed on the EU market, the CRA could have an impact on cybersecurity standards for such products beyond the EU borders. Indeed, non-EU operators might find it convenient to follow the CRA's rules as a default framework for their global operations instead of developing different products or processes for different markets.[14] Consequently, the EU might emerge as

---

8 Chiara Pier Giorgio, The Cyber Resilience Act: The EU Commission's Proposal for a Horizontal Regulation on Cybersecurity for Products with Digital Elements, International Cybersecurity Law Review 2022 (cit.: Chiara, Cyber Resilience Act), 256.

9 European Commission Staff Working Document, Impact Assessment Report accompanying the Document 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, SWD(2022) 282 final, 15 September 2022, part 1/3 (cit.: Impact Assessment Report, part 1), 1.

10 von der Leyen Ursula, 2021 State of the Union Address by President von der Leyen, September 2021, <https://ec.europa.eu/commission/presscorner/api/files/document/print/ov/speech_21_4701/SPEECH_21_4701_OV.pdf>.

11 Chiara, Cyber Resilience Act (fn 8), 255.

12 European Commission, Cyber Resilience Act: New EU Cybersecurity Rules Ensure More Secure Hardware and Software Products, September 2022, <https://data.europa.eu/doi/10.2759/543836>.

13 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, 15 September 2022 [hereinafter CRA or CRA Proposal].

14 Car Polona/De Luca Stefano, EU Cyber-resilience Act, European Parliamentary Research Service, PE 739.259, December 2022, 6.

the international reference point for cybersecurity of connected devices – triggering the so-called "Brussels effect" – similarly as in the area of data protection by means of the General Data Protection Regulation (GDPR).[15]

Following this brief introduction, the goal of this article is threefold: (1) to contextualize the CRA by outlining the drivers of its adoption against the broader picture of EU's role (and ambitions) in the cybersecurity domain as well as the EU's dynamic legislative landscape (Section B); (2) to provide an overview of the rules of the proposed CRA and critically evaluate selected aspects (Section C). Based on the analyses, we seek in the final Section (D) to assess whether and to what extent the CRA project would be successful in attaining its objectives and what the consequences of this could be.[16]

B. Drivers of a horizontal cybersecurity regulation

When examining the drivers of the proposed EU Cyber Resilience Act, it is apt to focus not only on the rationale of the regulatory initiative, namely the creation of an Internet of Secure Things, but to view this in the somewhat broader context of the EU's growing ambition to become a cybersecurity champion and its striving for digital sovereignty. We look in turn at these rationales behind the CRA in the next two sections.

I. Creating an Internet of Secure Things through harmonization and mandatory requirements

As stated at the outset, one of the focal points of cybersecurity challenges in the EU has been the Internet of Things, as its employment is characterized by a large number of vulnerabilities and a cross-border nature. This can potentially not only threaten the proper functioning of the internal market but also

---

15 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ (2016) L 119/1 [hereinafter GDPR].

16 It should be noted that the subsequent observations refer to the proposal of 15 September 2022. Discussions on this draft have meanwhile gained momentum in the Council of EU Ministers, and it is reported that the Swedish Presidency circulated a new compromise text on 27 January 2023, which was recently subject to discussion in the Horizontal Working Group on Cyber Issues, the technical body of the EU Council that prepares for adoption by the Ministers. See e.g., Bertuzzi Luca, EU Council Moves to Adjust Product Life-cycle, Reporting in New Cybersecurity Law, EURACTIV.com, 1 February 2023, <https://www.euractiv.com/section/cybersecurity/news/eu-council-moves-to-adjust-product-lifecycle-reporting-in-new-cybersecurity-law/> (cit.: Bertuzzi, February 2023).

fundamental rights and the security of EU citizens. Aware of this problematic interplay, the EU announced in its Cybersecurity Strategy for the Digital Decade[17] aiming to tackle this issue by inter alia incentivizing secure products and services in order to ensure an Internet of Secure Things.[18] One of the critical building blocks towards this goal is the proposed CRA.[19]

According to the CRA proposal, there are two major problems with respect to cybersecurity in products with digital elements: (1) products have low levels of cybersecurity; and (2) users are prevented from selecting products with adequate cybersecurity properties or using them in a secure manner due to insufficient understanding and access to information.[20]

1. Protecting consumers by imposing mandatory requirements for all connected devices

The first problem stems from the lack of incentives for manufacturers to take security seriously,[21] as well as the fierce competition from products coming at a much lower price, notably from China.[22] Indeed, although manufacturers of products with digital elements sometimes face reputational damage if their products are not secure enough, the costs of security breaches are mainly borne by consumers.[23] Besides, security vulnerabilities often do not lead users to actually switch products, due to the inherent network effects.[24] Consequently, manufacturers have little incentive to invest in the design and development of secure products and to provide security updates.[25] They also typically prioritize rapid market access through new feature development and compatibility with existing products over the development of security

17 Joint Communication to the European Parliament and the Council, The EU's Cybersecurity Strategy for the Digital Decade, JOIN(2020) 18 final, 16 December 2020 (cit.: EU's Cybersecurity Strategy for the Digital Decade).

18 EU's Cybersecurity Strategy for the Digital Decade (fn 17), 9.

19 Cf. Car/De Luca (fn 14), 2 et seq.

20 Recital 1 CRA Proposal.

21 Impact Assessment Report, part 1 (fn 9), 9.

22 Most infected IoT devices come from China and Taiwan, the world's leading hardware manufacturers. Rodríguez Elsa et al., Superspreaders: Quantifying the Role of IoT Manufacturers in Device Infections, 20th Annual Workshop on the Economics of Information Security WEIS 2021, <https://weis2021.econinfosec.org/wp-content/uploads/sites/9/2021/06/weis21-rodriguez.pdf>, 13.

23 European Economic and Social Committee, Opinion, Cyber Resilience Act, INT/999, adopted on 14 December 2022, 4.

24 Impact Assessment Report, part 1 (fn 9), 10.

25 European Economic and Social Committee (fn 23), 4.

properties.[26] Especially cheap devices exacerbate the issue, as they often stem from non-EU manufacturers that ship an entire series of products with a default password, such as 123456.[27]

Another important aspect is that the insecurity of devices is not just a local technical issue. Rather, such devices, notably sensors, are embedded in devices and systems that are managed by people who lack awareness of the potential vulnerabilities – for example, manufacturers of smart toys are familiar with the safe use of plastics but may lack awareness of cybersecurity and privacy threats to children.[28]

Additionally, users are often unaware of the security risks associated with products with digital elements and usually have no knowledge of a product's internal workings, so making purchasing decisions based on these features can be very difficult for them.[29] Accordingly, in many cases, cybersecurity incidents may be attributed to users selecting products that are inappropriate for their purposes or having hardware and software misconfigured,[30] thereby raising the security risk of their device or network unnecessarily.[31] The primary cause of this issue, as identified in the CRA Impact Assessment, is that manufacturers do not provide adequate information about security features, vulnerabilities, and how to use a device safely.[32] But even if users are familiar with the parameters of the product or service they purchase, they are unable to predict flaws that may show up later, especially since many vulnerabilities are only discovered years after a particular technology was developed. Also, the emergence of some vulnerabilities may not have been foreseeable at the time of product launch, as the assessment of the degree of security of a particular technology may change over time.[33]

---

26 Johnson et al. (fn 7), 706; Chiara, Cyber Resilience Act (fn 8), 256.

27 Gregersen Carsten Rhod, EU Cyber Resilience Act: The GDPR for IoT, embedded, 20 December 2022, <https://www.embedded.com/eu-cyber-resilience-act-the-gdpr-for-iot/#:~:text=The Cyber Resilience Act is,elements throughout their whole lifecycle>. According to Hernández-Ramos José L. et al., Toward a Data-Driven Society: A Technological Perspective on the Development of Cybersecurity and Data-Protection Policies, IEEE Security & Privacy 2020, 30, there is also the possibility that devices are put on the market that have default passwords, which are never changed during their life-cycle.

28 Carr/Lesniewska (fn 2), 397.

29 Impact Assessment Report, part 1 (fn 9), 10.

30 European Economic and Social Committee (fn 23), 4.

31 Impact Assessment Report, part 1 (fn 9), 8.

32 Impact Assessment Report, part 1 (fn 9), 14.

33 Banasinski Cezary/Rojszczak Marcin, Cybersecurity of Consumer Products against the Background of the EU Model of Cyberspace Protection, Journal of Cybersecurity 2021, 2.

In order to address the problem of low level of cybersecurity of products with digital elements marketed in the Union, the CRA imposes mandatory minimum-security requirements for all connected devices.[34] Against the problem of insufficient understanding among users and in order to enable organizations and consumers to use products with digital elements securely, the CRA proposal seeks to enhance transparency in various aspects.[35] The CRA essential cybersecurity requirements are also meant to contribute to strengthened protection of personal data and privacy of individuals. In this sense, cybersecurity is seen as a core element in the protection of fundamental rights and freedoms.[36]

2. Ensuring a coherent cybersecurity framework via horizontal regulation

The second driver behind the CRA adoption has been the fragmentation of the existing EU legal framework.[37] As a gap analysis study[38] showed, there is presently no piece of EU legislation that requires comprehensive cybersecurity requirements for all products with digital elements.[39] Rather, the current legislation comprises several sets of horizontal rules that address certain aspects linked to cybersecurity – yet from different angles.[40] While the Cybersecurity Act[41] as well as the Network and Information Security Directive (NIS Directive)[42] do come with measures to improve the security of the digital supply chain, they set no mandatory requirements for the security of products

34 Chiara, Cyber Resilience Act (fn 8), 257.

35 Impact Assessment Report, part 1 (fn 9), 21.

36 Chiara, Cyber Resilience Act (fn 8), 271.

37 Impact Assessment Report, part 1 (fn 9), 11.

38 Annex 13 of the Commission Staff Working Document, Impact Assessment Report, Annexes to the Impact Assessment Report accompanying the document 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, SWD(2022) 282 final, 15 September 2022, part 2/3.

39 Impact Assessment Report, part 1 (fn 9), 11.

40 Explanatory Memorandum to the CRA Proposal, 2.

41 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), OJ (2019) L 151/15 [hereinafter CSA].

42 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 (2016) L 194/1 [hereinafter NIS Directive].

with digital elements.[43] According to the CRA Impact Assessment this bears the risk of Member States adopting diverging national regulation.[44] Germany is a proof of this, having introduced first (non-binding) measures to enhance the security of products with digital elements.[45] Such initiatives may undermine the internal market, creating legal uncertainty for both manufacturers and users, as well as placing unnecessary burdens on economic operators to meet overlapping requirements for similar types of devices[46] – a state that is certainly not along the lines of the EU Strategy for a Digital Single Market.[47]

In order to avoid regulatory fragmentation and ensure a coherent cybersecurity framework, the CRA aims to streamline the EU's fragmented cybersecurity regulatory landscape by introducing horizontal cybersecurity requirements for products with digital elements.[48] The means of a Regulation over a Directive ensures this in a more immediate way and gives a level of legal certainty that a Directive, considering the leeway given for its implementation at the Member State level, could not achieve.[49]

II. Strengthening digital sovereignty via cybersecurity regulation

The CRA must also be seen in the context of concerted efforts of the EU to become a leading actor in the domain of cybersecurity and its interlinked striving, through a set of regulatory initiatives, to assert the EU's "digital sovereignty" and render it sustainable over time.

1. EU's cybersecurity activities

With regard to the former, it is evident that the last two decades have witnessed the emergence of cybersecurity as one of the most critical, as well as contentious, topics on regulatory agendas. This new strategic importance is intrinsically linked to the striving of various actors (states as well as international and supranational organizations) to shape and influence the

43 Recital 3 CRA Proposal.

44 Impact Assessment Report, part 1 (fn 9), 16 et seq.

45 Impact Assessment Report, part 1 (fn 9), 19.

46 Impact Assessment Report, part 1 (fn 9), 16 et seq.; Chiara, Cyber Resilience Act (fn 8), 257.

47 Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A Digital Single Market Strategy for Europe, COM(2015) 192 final, 6 May 2015.

48 Cf. Vikolainen Vera, Strengthening Cyber Resilience, European Parliament Research Service, PE 734.708, December 2022, 1.

49 Explanatory Memorandum to the CRA Proposal, 5.

governance of cyberspace.[50] Among them is the EU, for which cybersecurity is now one of the top priorities[51] and which aspires to position itself as a central cybersecurity actor.[52] EU's heightened prioritization of cybersecurity comes after a period of inaction, as, although the issue of safeguarding cyberspace has been on the EU institutional agenda for some 20 years now, almost no binding provisions were adopted.[53] Yet, against the backdrop of major cyberattacks and incidents, the EU accelerated its regulatory activity[54] and with the 2013 EU Cybersecurity Strategy[55] introduced cybersecurity as a new policy area.[56] The Cybersecurity Strategy is closely linked to the 2015 EU Digital Single Market Strategy as cybersecurity is an important instrument to prevent economic damage and enhance consumer trust.[57]

---

50 Backman Sarah, Risk vs. Threat-based Cybersecurity: The Case of the EU, European Security 2022, 1.

51 Carrapico Helena/Barrinha André, European Union Cyber Security as an Emerging Research and Policy Field, European Politics and Society 2018, 300.

52 Gao Xinchuchu/Chen Xuechen, Role Enactment and the Contestation of Global Cybersecurity Governance, Defence Studies 2022, 689.

53 Banasinski/Rojszczak (fn 33), 3. A comprehensive overview on how the topic of cybersecurity has evolved from its absence to its prominence on the European agenda is provided by Brandão Ana Paula/Camisão Isabel, Playing the Market Card: The Commission's Strategy to Shape EU Cybersecurity Policy, JCMS 2022, 1339 et seqq.

54 Today there are numerous EU legal instruments relevant to cybersecurity and given that cybersecurity is a cross-cutting issue, there are not only laws on information society and cyber resilience, but also EU legal acts on cyber deterrence and defense. Given the limited space, in the following only selected policies are highlighted. For more details on the cybersecurity regulatory landscape, cf.: Kasper Agnes/Antonov Alexander, Towards Conceptualizing EU Cybersecurity Law, ZEI Discussion Paper 2019, <https://www.zei.uni-bonn.de/de/publikationen/medien/zei-dp/zei-dp-253-2019.pdf>; European Court of Auditors, Challenges to Effective EU Cybersecurity Policy, Briefing Paper, March 2019, <https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_EN.pdf>, 9; Wessel Ramses A., Cybersecurity in the European Union: Resilience through Regulation?, in: Conde Elena/Yaneva Zhaklin/Scopelliti Marzia (eds.), Routledge Handbook of EU Security Law and Policy, Abingdon 2019.

55 Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, JOIN(2013) 1 final, 7 February 2013.

56 Fuster Gloria González/Jasmontaite Lina, Cybersecurity Regulation in the European Union: The Digital, the Critical and Fundamental Rights, in: Christen Markus/Gordijn Bert/Loi Michele (eds.), The Ethics of Cybersecurity, Cham 2020, 98.

57 Bendiek Annegret/Pander Maat Eva, The EU's Regulatory Approach to Cybersecurity, German Institute for international and Security Affairs, WP NR. 02 2019, <https://www.swp-berlin.org/publications/products/arbeitspapiere/WP_Bendiek_Pander_Maat_EU_Approach_Cybersecurity.pdf>, 4 et seq.

The main pillar of the 2013 Cybersecurity Strategy was the NIS Directive that came into effect in 2016 and was the first EU-wide horizontal instrument, i.e., cross-sectoral instrument, to regulate cybersecurity.[58] The NIS Directive aimed to ensure a high level of network and information security at the EU level by setting security and incident reporting obligations for operators of essential services and digital service providers,[59] as well as achieve a minimum level harmonization across the Member States.[60] The GDPR, adopted also in 2016, approaches cybersecurity from the angle of data protection, and sets out technical requirements for security of personal data and a breach notification regime.[61]

The second Cybersecurity Strategy was proposed in 2017[62] and resulted in the proposal for the EU Cybersecurity Act, which was adopted on 12 March 2019.[63] The Cybersecurity Act was a significant step forward in the EU's approach to cybersecurity as it introduced an EU-wide cybersecurity certification framework for products and services as well as granted the European Union Agency for Cybersecurity (ENISA) a permanent mandate.[64] The follow-up and presently applying "Cybersecurity Strategy for the Digital Decade" of 2020 focuses on three areas: (1) resilience, technological sovereignty and leadership; (2) operational capacity to prevent, deter and respond; (3) a global and open cyberspace. The revised NIS Directive (NIS2 Directive),[65] which entered into

---

58 Markopouloua Dimitra/Papakonstantinou Vagelis/De Hert Paul, The New EU Cybersecurity Framework: The NIS Directive, ENISA's Role and the General Data Protection Regulation, Computer Law & Security Review 2019, 1; Schmitz-Berndt Sandra/Cole Mark D., Towards an Efficient and Coherent Regulatory Framework on Cybersecurity in the EU: The Proposals for a NIS 2.0 Directive and a Cyber Resilience Act, ACIG 2022, 5.

59 Carrapico/Barrinha (fn 51), 300; Hernández-Ramos et al. (fn 27), 32.

60 European Court of Auditors (fn 54), 13.

61 Arts. 32–34 GDPR. Kasper/Antonov (fn 54), 34; Bederna Zsolt/Rajnai Zoltan, Analysis of the Cybersecurity Ecosystem in the European Union, International Cybersecurity Law Review 2022, 39 et seq. A comprehensive overview of the cybersecurity obligations of the GDPR provide Mantelero Alessandro et al., The Common EU Approach to Personal Data and Cybersecurity Regulation, International Journal of Law and Information Technology 2020, 306.

62 Joint Communication to the European Parliament and the Council, Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, Brussels, JOIN(2017) 450 final, 13 September 2017.

63 Chiara Pier Giorgio, The IoT and the New EU Cybersecurity Regulatory Landscape, International Review of Law, Computers & Technology 2022 (cit.: Chiara, IoT), 119 et seq.

64 Bendiek/Pander (fn 57), 12 et seq.; Hernández-Ramos et al. (fn 27), 32.

65 Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 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), OJ (2022) L 333/80 [hereinafter NIS2 Directive].

force in January 2023, accordingly aims to enhance the level of cyber resilience by requiring all public and private entities across the single market that perform important functions for the economy and society as a whole to adopt appropriate cybersecurity measures. It also seeks to strengthen the cyber-security risk management and improve cooperation between the relevant competent authorities.[66]

Importantly, the Cybersecurity Strategy for the Digital Decade also announced new horizontal rules to improve the cybersecurity of products with digital elements. This triggered the legislative process[67] and ultimately led to the Commission's CRA proposal of 15 September 2022.[68] The CRA forms part of a large number of EU legal acts in the digital domain, such as on AI, data spaces, online platforms, that affect but also go beyond cybersecurity.[69] This regulatory activism can be well understood in the context of the EU's pursuit of "digital sovereignty", also dubbed as a process of "re-sovereignization".[70]

2. Digital sovereignty and EU's re-sovereignization

The term "digital sovereignty" expresses the idea that "states should reassert their authority over the internet and protect their citizens and businesses from the manifold challenges to self-determination in the digital sphere."[71] Yet, the term lacks a uniform definition and is used inconsistently in EU policy documents. Indeed, even essential elements are unclear, such as whether digital sovereignty is something that the EU already possesses, or whether it is a goal that the EU should aspire to.[72] Nevertheless, the term "sovereignty" has been increasingly used since 2019, notably by Ursula von der Leyen's

---

66 Bederna/Rajnai (fn 61), 39 et seq.; Schmitz-Berndt Sandra, Cybersecurity Is Gaining Momentum - NIS 2.0 Is on Its Way, European Data Protection Law Review 2021, 582 et seq.

67 Council of the European Union, Council conclusions on the development of the European Union's cyber posture - Council conclusions approved by the Council at its meeting on 23 May 2022, Brussels, 23 May 2022, 6.

68 Further on the legislative history of the CRA: Car/De Luca (fn 14), 4 et seqq.

69 Codagnone Cristiano/Weigl Linda, Leading the Charge on Digital Regulation: The More, the Better, or Policy Bubble?, Digital Society 2023, 7 et seq.

70 Bendiek Annegret/Stürzer Isabella, Advancing European Internal and External Digital Sovereignty: The Brussels Effect and the EU-US Trade and Technology Council, German Institute for international and Security Affairs, SWP Comment 2022, <https://www.swp-berlin.org/publications/products/comments/2022C20_EuropeanDigitalSovereignty.pdf>, 8.

71 Pohle Julia/Thiel Thorsten, Digital Sovereignty, Internet Policy Review 2020, 2.

72 Roberts Huw et al., Safeguarding European Values with Digital Sovereignty: An Analysis of Statements and Policies, Internet Policy Review 2021, 12.

Geopolitical Commission, which urged the EU to be at the forefront of key technologies and future-proof infrastructure, with common standards, gigabit networks and secure current and next-generation clouds.[73] The President of the European Council, Charles Michel, has also constructed digital sovereignty as a strategy, in the sense that the EU sets its own rules, makes autonomous technological choices and develops its own digital solutions.[74] Similarly, the European Commission has announced the years 2020–2030 as Europe's "digital decade" and stated that securing Europe's "technological sovereignty" and "digital sovereignty" are key strategic objectives during this period.[75]

Cybersecurity appears as a core pillar of the EU's digital sovereignty, as strong cybersecurity is seen as a prerequisite for other policy areas, since the security of data, infrastructure and economic entities are necessary for a functional and competitive EU digital economy as well as for the safeguarding of EU values.[76] Consequently, there are various legislative initiatives that seek to strengthen the EU's digital sovereignty by making it a standard-setter in the field of cybersecurity,[77] such as the above-mentioned NIS2 Directive, the Cybersecurity Act as well as the GDPR, together with the EU Cybersecurity Strategy, which highlights the need for technological sovereignty too. The CRA only adds to this package, in particular in the domain of cybersecurity standard-setting for all products with digital elements.

In this context and making the link to the "Brussels effect", whereby the EU, as a regulatory superpower, "exports" its standards and they become the global ones,[78] the CRA can arguably be seen as the "GDPR for IoT".[79] If this effect, in analogy to global data protection, eventually materializes would very much depend on the level and type of obligations, the material

---

73 von der Leyen Ursula, Speech in the European Parliament Plenary Session, November 2019, <https://ec.europa.eu/commission/presscorner/api/files/attachment/858838/Speech by President-elect von der Leyen at the EP - as delivered in EN-FR-DE.pdf>, 9.

74 Barrinha André/Christou George, Speaking Sovereignty: The EU in the Cyber Domain, European Security 2022, 362.

75 Bendiek Annegret/Stürzer Isabella, The Brussels Effect, European Regulatory Power and Political Capital: Evidence for Mutually Reinforcing Internal and External Dimensions of the Brussels Effect from the European Digital Policy Debate, Digital Society 2023, 4.

76 Roberts et al. (fn 72), 12.

77 Madiega Tambiama, Digital Sovereignty for Europe, European Parliamentary Research Service, PE 651.992, July 2020, 4; Barrinha/Christou (fn 74), 429.

78 Anu Bradford, The Brussels Effect, Northwestern University Law Review (2012), 1; Anu Bradford, The Brussels Effect: How The European Union Rules the World, Oxford 2020; Fahey Elaine, EU as a Global Digital Actor: Institutionalising Global Data Protection, Trade, and Cybersecurity, London 2022.

79 Gregersen (fn 27).

scope and extra-territorial reach of the CRA, its stringency of monitoring and enforcement, among other things.[80] The "Brussels effect", although admittedly not a form of international cooperation but a case of unilateral standard-setting, could also have positive impact – in that it "may ultimately contribute to the enhancement of global cyber resilience".[81]

The following section looks more closely at key aspects of the proposed CRA, which gives us also the basis to test to what extent the regulatory rationales driving the CRA's adoption find an appropriate reflection in its legal provisions and contribute to EU's digital sovereignty and the multiplication of the "Brussels effect".

C. The proposed Cyber Resilience Act: Analysis of selected key aspects

Consisting of 71 Recitals, 57 Articles and 6 Annexes (for an overview, see Table 1 below), the proposed Cyber Resilience Act aims to create a coherent cybersecurity framework by requiring that products with digital elements are secure along the supply chain and throughout their life-cycle, as well as by enabling users to take cybersecurity into account when selecting and using products with digital elements.[82]

The CRA subject matter consists of four general elements, listed in Art. 1: (1) rules for the placing on the market of products with digital elements to ensure the cybersecurity of such products; (2) essential requirements for the design, development and production of products with digital elements, and obligations for economic operators in relation to these products with respect to cybersecurity; (3) 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, and obligations for economic operators in relation to these processes; and (4) rules on market surveillance and enforcement of the above-mentioned rules and requirements.

---

80 Bendiek/Pander (fn 57), 8.

81 Saalman Lora/Su Fei/Saveleva Dovgal Larisa, Cyber Posture Trends in China, Russia, the United States and the European Union, December 2022, <https://www.sipri.org/sites/default/files/2022-12/2212_cyber_postures_0.pdf>, 22.

82 Council of the European Union, 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) 2019/102 - Progress Report, 18 November 2022 (cit.: Council of the European Union, Progress Report), 2.

However, these elements cannot be allocated to individual chapters of the regulation. Yet, it may be difficult to link these core regulatory elements with discrete chapters and/or annexes of the CRA. Rather, these aspects recur throughout the entire regulation, including the Annexes, and the related rights and obligations need to be taken as appropriately together. The chapters of the proposed CRA and its Annexes are structured as follows:

Chapter I: General Provisions	Arts. 1 – 9
Chapter II: Obligations of Economic Operators	Arts. 10 – 17
Chapter III: Conformity of the Product with Digital Elements	Arts. 18 – 24
Chapter IV: Notification of Conformity Assessment Bodies	Arts. 25 – 40
Chapter V: Market Surveillance and Enforcement	Arts. 41 – 49
Chapter VI: Delegated Powers and Committee Procedure	Arts. 50 – 51
Chapter VII: Confidentiality and Penalties	Arts. 52 – 53
Chapter VIII: Transitional and Final Provisions	Arts. 54 – 57

Annex I: Essential Cybersecurity Requirements

1. Security Requirements Relating to the Properties of Products with Digital Elements
2. Vulnerability Handling Requirements

Annex II: Information and Instructions to the User

Annex III: Critical Products with Digital Elements

Annex IV: EU Declaration of Conformity

Annex V: Contents of the Technical Documentation

Annex VI: Conformity Assessment Procedures

- Conformity Assessment Procedure Based on Internal Control (Based on Module A)
- EU-type Examination (Based on Module B)
- Conformity to Type Based on Internal Production Control (Based on Module C)
- Conformity Based on Full Quality Assurance (Based on Module H)

Table 1: Overview of the CRA's chapters and annexes

In the following, we analyze in more detail: (1) the nature and scope of the CRA; (2) the risk-based classification of products; (3) the economic operators' obligations; (4) the monitoring and enforcement mechanism; and (5) the fines for non-compliance.

I. Horizontal regulatory intervention with a broad scope of application

1. Regulatory intervention based on Art. 114 TFEU

Art. 114 of the Treaty on the Functioning of the European Union (TFEU)[83] gives the legal basis for the CRA.[84] This is linked to the now common practice of using the catch-all provision of Art. 114 TFEU, i.e., the political and legal mandate to regulate the internal market, to adopt policies and legislation on cybersecurity.[85] This path is aptly chosen, given that cybersecurity remains a legal competence of the Member States and the EU constitutional law provides no unified legal basis for the Union to regulate cybersecurity.[86] The market-security nexus opens a door for the EU legislator in the cybersecurity context and this has been the case also with NIS Directive.[87] While there is no jurisprudence specifically on cybersecurity, the CJEU has confirmed internal market regulation as the proper legal basis for regulating cyberspace.[88]

Views on the soundness of this approach differ. Some authors have referred to this interventionist top-down approach, especially in the field of technology regulation, that introduces new concepts, principles and governmental mechanisms into the legal systems of the Member States, as "regulatory brutality"[89] that is likely to ignore Member States' particularities and is not

---

83 Consolidated version of the Treaty on the Functioning of the European Union, OJ (2012) C 326/47, 26 October 2012.

84 Explanatory Memorandum to the CRA Proposal, 3 et seq.

85 Miadzvetskaya Yuliya/Wessel Ramses A., The Externalisation of the EU's Cybersecurity Regime: The Cyber Diplomacy Toolbox, European Papers 2021, 419.

86 Bendiek/Pander (fn 57), 3; Wessel Ramses A., European Law and Cyberspace, in: Tsagourias Nicholas/Buchan Russell (eds.), Research Handbook on International Law and Cyberspace, Cheltenham 2021.

87 Brandão/Camisão (fn 53), 1338; Fuster/Jasmontaite (fn 56), 107.

88 Bendiek/Pander (fn 57), 7; Miadzvetskaya/Wessel (fn 85), 419; cf. Case C-217/04 United Kingdom vs. European Parliament and Council ECLI:EU:C:2006:279 and Joined Cases C-293/12 and C-594/12 Digital Rights Ireland Ltd ECLI:EU:C:2014:238.

89 Papakonstantinou Vagelis/De Hert Paul, The Regulation of Digital Technologies in the EU: The Law-making Phenomena of "actification", "GDPR mimesis" and "EU law brutality", TechReg 2022, 56.

about harmonization but rather about implanting of entirely new regimes. With regard to the CRA, such a deep type of intervention – as will be shown in more detail below – is likely to occur in some but not all affected domains.

2. Extensive material scope

The proposed CRA comes with a wide material scope as it applies 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."[90] "Products with digital elements" are defined as "any software or hardware product and its remote data processing solutions, including software or hardware components to be placed on the market separately."[91] Due to the use of "or", the definition of "products with digital elements" can be read to include software as a separate product from the hardware.[92] This reading seems to be confirmed by Recital 46 CRA, which refers to "software products" as well as by the fact that, according to the Explanatory Memorandum, non-embedded software is also covered, as it is often exposed to vulnerabilities.[93]

Furthermore, the CRA seems to not only encompass "finished" software and hardware products but also components thereof, as Art. 3(2) also refers to "software and hardware components to be placed on the market separately". Accordingly, the scope of protection not only covers end devices like smartphones, smart speakers, sensors, smart meters, routers, industrial control systems as well as software like desktop applications, video games and operating systems but also components such as computer processing units (CPUs) and software libraries.[94] Covered are also artificial intelligence (AI) systems, including products with digital elements that are classified as high-risk AI systems.[95]

Overall, the CRA's scope of application is very broad and basically all products with digital elements are covered.[96] This appears well justified since potentially all products with digital elements integrated in or connected to a larger electronic information system can serve as an entry point for attack by

---

90 Art. 2(1) CRA Proposal.

91 Art. 3 point (1) CRA Proposal.

92 Chiara, Cyber Resilience Act (fn 8), 258.

93 Explanatory Memorandum to the CRA Proposal, 7.

94 Impact Assessment Report, part 1 (fn 9), 2.

95 Car/De Luca (fn 14), 6.

96 European Economic and Social Committee (fn 23), 2; Chiara, Cyber Resilience Act (fn 8), 257 et seq.

malicious actors,[97] and that vulnerabilities are found not only in end products, but also in intermediate software components.[98] Despite subscribing to this all-encompassing approach along the lines of "[c]ybersecurity of the entire ecosystem is ensured only if all its components are cyber-secure,"[99] the European Commission also takes into account that not all products with digital elements are equally critical and therefore introduces a graduated series of obligations, as shown below.

Some products are also explicitly excluded from the CRA's scope of application. First of all, the CRA does not apply to products with digital elements that already fall under specific sectoral regulation with corresponding cybersecurity requirements,[100] such as medical devices[101] and in vitro diagnostic medical devices,[102] as well as products covered by the Vehicle General Safety Regulation[103] and the Regulation on common rules in civil

97 Cf. Recital 7 CRA Proposal.

98 Cf. Impact Assessment Report, part 1 (fn 9), 7.

99 Explanatory Memorandum to the CRA Proposal, 2.

100 Cf. Recitals 12 and 13 and Art. 2(2 and 3) CRA Proposal; Chiara, Cyber Resilience Act (fn 8), 259.

101 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, OJ (2017) L 117/1.

102 Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU, OJ (2017) L 117/176.

103 Regulation (EU) 2019/2144 of the European Parliament and of the Council of 27 November 2019 on type-approval requirements for motor vehicles and their trailers, and systems, components and separate technical units intended for such vehicles, as regards their general safety and the protection of vehicle occupants and vulnerable road users, amending Regulation (EU) 2018/858 of the European Parliament and of the Council and repealing Regulations (EC) No 78/2009, (EC) No 79/2009 and (EC) No 661/2009 of the European Parliament and of the Council and Commission Regulations (EC) No 631/2009, (EU) No 406/2010, (EU) No 672/2010, (EU) No 1003/2010, (EU) No 1005/2010, (EU) No 1008/2010, (EU) No 1009/2010, (EU) No 19/2011, (EU) No 109/2011, (EU) No 458/2011, (EU) No 65/2012, (EU) No 130/2012, (EU) No 347/2012, (EU) No 351/2012, (EU) No 1230/2012 and (EU) 2015/166, OJ (2019) L 325/1.

aviation.[104] The European Data Protection Supervisor (EDPS) has noted however that the Regulation on medical devices is not detailed and specific enough to meet the cybersecurity standards of the CRA, contrary to what is purported in Recital 12 CRA. The EDPS thus recommends that this particular Regulation should be deleted from the list of legislation excluded from the scope of the CRA.[105]

Additionally, Art. 2(5) CRA excludes products with digital elements developed exclusively for national security or military purposes and products specifically designed to process classified information from its scope of application. However, a large share of products used in the defence sector are civil and dual-use products with digital elements[106] and are accordingly subject to the CRA.

A further exception can be found in Recital 10 CRA, which stipulates that "free and open source software developed or supplied outside the course of a commercial activity" should not be covered by the CRA to avoid hampering innovation and research. While the objective of this exemption is to be welcomed, it merits clarity. First of all, the CRA does not define relevant terms such as "free software", "open source software" and "free and open source software".[107] Further is the scope of "commercial activity" unclear as according to Recital 10, a commercial activity can be characterized not only by charging a price for a product but for instance also by charging a price for technical support services. Should the scope of Recital 10 CRA remain unclear, there are concerns that the certification process and the fines that could be applied under the adopted CRA could impede the development of open source software and cause open source products to be withdrawn from the internal

---

104 Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and amending Regulations (EC) No 2111/2005, (EC) No 1008/2008, (EU) No 996/2010, (EU) No 376/2014 and Directives 2014/30/EU and 2014/53/EU of the European Parliament and of the Council, and repealing Regulations (EC) No 552/2004 and (EC) No 216/2008 of the European Parliament and of the Council and Council Regulation (EEC) No 3922/9, OJ (2018) L 212/1.

105 European Data Protection Supervisor, Opinion 23/2022 on the 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, November 2022, <https://edps.europa.eu/system/files/2022-11/2022-0921_d2649_opinion_en.pdf>, 8.

106 High Representative of the Union for Foreign Affairs and Security Policy, Joint Communication to the European Parliament and the Council, EU Policy on Cyber Defence, JOIN(2022) 49 final, 10 November 2022, 11.

107 European Data Protection Supervisor (fn 105), 10.

market, which could affect innovation in Europe.[108] Yet, it should be borne in mind that often commercial software relies on open source components and such components might exhibit vulnerabilities,[109] just as recently seen with Log4Shell, a zero-day vulnerability in Log4j.[110] The open source library Log4j is used by many major software manufacturers and the vulnerability thus led to security incidents around the world.[111] It is therefore necessary to formulate an exception that provides clarity as well as an appropriate balance in terms of responsibility.

Another exception is formulated in Recital 9 CRA. It indicates that Software-as-a-Service (SaaS) is not covered by the CRA, except for "remote data processing solutions relating to a product with digital elements". This exception is intended to ensure that there is no overlap resulting from SaaS already covered by the NIS2 Directive and the catch-all scope of application of the CRA.[112] However, as products that rely on "remote data processing" are not excluded by Recital 9, it is possible that SaaS is nonetheless, at least partially, included in CRA's scope, given that virtually all SaaS products rely on "remote data processing".[113] Clarification in this respect seems to be underway, as it is reported that the new version of the CRA text from the Czech presidency, dated 2 December 2022, clearly excludes SaaS from the scope of the CRA.[114] The text also clarifies that websites would not qualify as remote data processing solutions of web browsers, because they are not developed under the control of the browser manufacturer, and the browser would not be prevented from functioning if single website were absent.[115]

---

108 Car/De Luca (fn 14), 9; Ilkka Turunen, Europe's Cyber Security Strategy Must Be Clear about Open Source, Computer Weekly.com, 12 January 2023, <https://www.computerweekly.com/opinion/Europes-cyber-security-strategy-must-be-clear-about-open-source>.

109 Kazakova Anastasiya/Kumagin Igor, The EU's Upcoming Cyber Resilience Act Should Set New Rules for the Game, June 2022, <https://www.kaspersky.com/about/policy-blog/index/the-eus-upcoming-cyber-resilience-act-should-set-new-rules-for-the-game>.

110 Wortley Free/Thompson Chris/Allison Forrest, Log4Shell: RCE 0-Day Exploit Found in log4j, a Popular Java Logging Package, December 2021, <https://www.lunasec.io/docs/blog/log4j-zero-day/>.

111 Impact Assessment Report, part 1 (fn 9), 7.

112 Explanatory Memorandum to the CRA Proposal, 2 et seq.

113 Chiara, Cyber Resilience Act (fn 8), 259.

114 Bertuzzi Luca, EU Council Moves to Exclude Software-as-a-Service from New Cybersecurity Law, EURACTIV.com, 9 December 2022, <https://www.euractiv.com/section/cybersecurity/news/eu-council-moves-to-exclude-software-as-a-service-from-new-cybersecurity-law/> (cit.: Bertuzzi, December 2022).

115 Bertuzzi, December 2022 (fn 114).

Overall, more clarification on the scope of the proposal is clearly needed[116] and this is likely to be addressed in the next legislative steps of adopting the CRA.

3. Complex interplay with other regulations

The above definitional dilemmas are also indicative of the problem that, due to the broad scope of the CRA, there may be overlaps with other laws in the field and the respective scopes of application may not be clearly distinguishable from one another. As the CRA is seen as "the missing piece of the puzzle completing the picture of EU cybersecurity policies",[117] it is critical that it dovetails with the existing as well as the proposed legislation in the digital domain addressing products' cybersecurity, either directly or indirectly.

The interplay between the CRA and other legislation prescribing cybersecurity requirements for products with digital elements is addressed by Art. 2(4).[118] Next to the above-mentioned exemptions, Art. 2(4) can be seen as operationalizing "a rule of prevalence", as it provides criteria to determine whether other legal acts, which address all or some of the risks covered by the essential requirements laid down in Annex I of the CRA, may prevail over the CRA.[119] Having some criteria in place is paramount in light of the fact that Recital 14 states that sectoral or product-specific Union legislation may be introduced – i.e., there is a possibility that after enactment of the CRA, further sector-specific legislation may follow, whose interplay with the CRA would need to be clarified.

The CRA does provide also explicit guidance on its interplay with certain existing pieces of legislation – such as the Cybersecurity Act, the NIS2 Directive, the GDPR, as well as the proposed AI Act[120]. In relation to the Cybersecurity Act, the CRA aims to exploit synergies mainly with regard to the conformity assessment process.[121] Pursuant to Article 18(3) and (4) CRA, the relationship between the CRA and the Cybersecurity Act is such that

---

116 Council of the European Union, Progress Report (fn 82), 5.

117 Impact Assessment Report, part 1 (fn 9), 4.

118 Chiara, Cyber Resilience Act (fn 8), 266.

119 Chiara, Cyber Resilience Act (fn 8), 266. According to Art. 2(4) the application of the CRA may be limited or excluded where such a limitation or exclusion is consistent with the overall regulatory framework applying to those products and if the sectoral rules achieve the same level of protection as the one provided for by the CRA.

120 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, 21 April 2021 [hereinafter AI Act].

121 Car/De Luca (fn 14), 8.

digital products that comply with the voluntary cybersecurity certification schemes are deemed to comply with the CRA's conformity assessment.[122] With respect to the NIS2 Directive, the CRA intends to complement it in that it seeks to make it easier for digital infrastructure providers to meet the supply chain requirements under the NIS2 Directive by ensuring that the products with digital elements that they use to deliver their services are developed in a secure manner and that they have access to timely security updates for those products.[123] Similarly to the NIS2 Directive, the CRA aims to complement the GDPR[124] and exploit synergies. Pursuant to Recital 17, the CRA should be without prejudice to the GDPR. Rather the CRA is intended to contribute to the protection of personal data and privacy of individuals and to create synergies in both standardization and certification on cybersecurity, as well as in the area of market surveillance and enforcement.[125] However, the EDPS has observed that the governance provisions of Recital 17 are not fully mirrored in the operative part of the CRA. In the absence of clear provisions, the EDPS is concerned that synergies are unlikely to be achieved in practice and recommends inter alia specifying the synergies between the CRA and the GDPR in the area of market surveillance and enforcement.[126]

Finally, with respect to the proposed AI Act the general rule is that for products with digital elements covered by the CRA that are simultaneously classified as "high-risk AI systems" under the AI proposal, the CRA's conformity assessment procedure shall apply to demonstrate their compliance with the security requirements of the proposed AI Act.[127] Exceptions apply for certain AI critical products.[128]

There are further provisions on the CRA's interface[129] that include: clarification on the interplay between the CRA and the General Product Safety Regulation

---

122 Car/De Luca (fn 14), 8.

123 Recital 11 CRA Proposal. For more details: Chiara, Cyber Resilience Act (fn 8), 270 and Schmitz-Berndt/Cole (fn 58), 12 et seq.

124 For general observations on the relationship between cybersecurity and data protection, cf. Kuner Christopher et al., The Rise of Cybersecurity and Its Impact on Data Protection, International Data Privacy Law 2017, 73.

125 Recital 17 CRA Proposal.

126 European Data Protection Supervisor (fn 105), 8.

127 Art. 8 and Recital 29 CRA Proposal; European Economic and Social Committee (fn 23), 3.

128 Car/De Luca (fn 14), 8.

129 Besides the ones mentioned, there are also some provisions in Recitals 30 and 31 CRA Proposal.

(Art. 7);[130] CRA's interface with the Machinery Regulation Proposal (Art. 9);[131] and with the Delegated Act to the Radio Equipment Directive (RED) (Recital 15).[132]. As regards the latter, it should be noted that to avoid a regulatory overlap, it is planned that the Commission would repeal or amend the RED delegated regulation with respect to the radio equipment covered by the CRA, so that the latter one would apply to it.[133]

Yet, despite all these clarifications on the interplay with other regulations one can find in the CRA, there is a possibility that its broad horizontal scope will not straightforwardly lead to a streamlined regulatory landscape. Given the complex legal landscape, and considering that further regulations are in the making, it would be desirable that the Commission develops guidelines to provide better guidance to manufacturers and consumers on the exact rules and procedures that apply in practice.[134] Otherwise, there is a risk that the CRA will fall short of its objective for coherent regulation by merely adding an additional layer of requirements, thereby making it even more complicated for addressees to navigate the legislative landscape and exacerbating the problems that it is indeed intended to tackle.[135]

4. Addressees along the supply chain

The CRA not only has a wide scope of material application, but also its personal scope is comprehensive, as the CRA addresses all market participants involved in the supply chain: from manufacturers to distributors and importers.[136] This is new and remarkable in the field of EU cybersecurity law.[137] Depending on the classification as either manufacturer, importer or distributor, economic operators are subject to different obligations,[138] which are discussed below.

---

130 For more details: Chiara, Cyber Resilience Act (fn 8), 267.

131 For more details: Chiara, Cyber Resilience Act (fn 8), 268.

132 For more details: Chiara, Cyber Resilience Act (fn 8), 268.

133 Explanatory Memorandum to the CRA Proposal, 4.

134 Cf. European Economic and Social Committee (fn 23), 1.

135 Cf. Digitaleurope, Building Blocks for a Scalable Cyber Resilience Act, May 2022, <https://digital-europe-website-v1.s3.fr-par.scw.cloud/uploads/2022/05/Building-blocks-for-a-scalable-Cyber-Resilience-Act.pdf>, 5.

136 Cf. Art. 3 point (17) CRA Proposal.

137 Chiara, Cyber Resilience Act (fn 8), 260; Kipker Dennis-Kenji, Der EU "Cyber Resilience Act" kommt – und mit ihm die umfassendsten Compliance-Pflichten in der IT-Sicherheit, die es jemals gab, MMR-Aktuell 2022.

138 Section C.III.

According to Art. 3(18) CRA, a manufacturer is a natural or legal person who develops or manufactures a product with digital elements himself, or who has such products designed, developed or manufactured by third parties and then markets these products under his own name or trademark, irrespective of whether this is done for a fee or free of charge.[139] An importer is a natural or legal person established in the EU who places on the market a product with digital elements that bears the name or trademark of a natural or legal person established outside the EU.[140] "Placing on the market" means thereby the first making available on the Union market.[141] A natural or legal person in the supply chain, other than the manufacturer or the importer, that supplies product with digital elements for distribution or use on the Union market in the course of a commercial activity without affecting the devices properties is deemed to be a distributor.[142]

It should be noted that the CRA, like other cybersecurity legislation,[143] does not grant rights to individuals and they are not addressees of the regulation. However, users may still fall within the scope of the CRA. This is the case if Art. 16 CRA comes into play. This provision stipulates that a "natural or legal person, other than the manufacturer, the importer or the distributor, that carries out a substantial modification of the product with digital elements shall be considered a manufacturer". "Substantial modifications" are any changes to the product that affect the product's compliance with the essential cybersecurity requirements of Section 1 of Annex I, or results in a change of its intended use.[144] Pursuant to Recital 24 refurbishing, maintaining as well as repairing a product with digital elements are not to considered as substantial modifications, as long as the intended use and functionalities remain unchanged and the level of risk unaffected. Yet, if functional upgrades are made in the course of these activities, a substantial change may occur.[145] So to put it simply, if users (be it natural or legal persons) elevate themselves to a position similar to the role of manufacturer by making substantial changes to a product they may be subject to individual manufacturer obligations.[146] The consequence of this is that the person is, pursuant to Art. 16 CRA, "subject to

139 Art. 3 point (18) CRA Proposal.

140 Art. 3 point (20) CRA Proposal.

141 Art. 3 point (22) CRA Proposal.

142 Art. 3 point (21) CRA Proposal in connection with Art. 3 point (23) CRA Proposal.

143 Cf. Markopouloua/Papakonstantinou/De Hert (fn 58), 11.

144 Art. 3 point (31) CRA Proposal.

145 Zirnstein Yannick, Der Entwurf des Cyber Resilience Act, Computer und Recht 2022, 711 et seq.

146 Zirnstein (fn 145), 711.

the obligations of the manufacturer set out in Articles 10 and 11(1), (2), (4) and (7), for the part of the product that is affected by the substantial modification or, if the substantial modification has an impact on the cybersecurity of the product with digital elements as a whole, for the entire product". Bearing in mind the burdensome obligations the manufacturer has to fulfil[147] and the heavy fines that can be imposed in the case of non-compliance,[148] as well as the consumer protection rationale inherent in the CRA, one can reasonably ask if Art. 16 goes too far.[149] Some of this excess possibility seems acknowledged by the CRA, as it states in Recital 66 that when fining persons, their economic situation as well as the general level of income in the respective Member State should be taken into account.

5. CRA's territorial scope

The CRA does not contain any explicit provisions on the territorial scope of its application.[150] However, the various references to products with digital elements that are "placed on the EU market" or "made available on the market" indicate that the CRA applies to such products that are offered for sale or use in the Union.[151] In particular Art. 1(a) states that the CRA lays down "rules for the placing on the market for products with digital elements".[152] "Placing on the market" means making available on the EU market for the first time, which is the supply of a product with digital elements for distribution or use on the EU market in the course of a commercial activity, regardless of whether this is done for payment or free of charge.[153] It appears that it is this particular link with the EU market that triggers the CRA's application.

At the same time, if one looks at the various definitions of the different economic operators, it is noticeable that the definition of the manufacturer,

147 Section C.III.1.

148 Section C.V.

149 Cf. Zußner Matthias, Das Inverkehrbringen von Produkten mit digitalen Elementen nach dem Vorschlag der EU-Kommission für eine Verordnung über horizontale Cybersicherheitsanforderungen, Austrian Law Journal 2022, 196 et seq.

150 Zirnstein (fn 145), 709.

151 Tuninetti Ferrari Andrea et al., EU Cyber Resilience Act - Proposed Cyber-Security Rules for Connected Products, Clifford Chance Briefing, November 2022, <https://www.cliffordchance.com/content/dam/cliffordchance/briefings/2022/11/EU-Cyber-Resilience-Act-Proposed-Cyber-Security-Rules-for-Connected-Products.pdf>, 2.

152 In the same sense Recital 1 reads: "It is necessary to improve the functioning of the internal market by laying down a uniform legal framework for essential cybersecurity requirements for placing products with digital elements on the Union market."

153 Art. 3 point (22) and (23) CRA Proposal.

unlike that of importer and distributor, does not make reference to the Union. According to Zirnstein, this is an indication that the CRA strives for an extra-territorial application since although manufacturers could disregard the CRA's safety requirements if they are based outside the Union, importers would not be allowed to import any of these products into the European market, as they must attest that manufacturers' products ensure compliance with the requirements of Annex I CRA. In other words, the scope of the Regulation extends beyond the EU borders as any manufacturer based outside the EU exporting to EU Member States is subject to the legislation in the sense that its importer and (less so) distributor are liable for their compliance.[154]

Given that the CRA is likely to also apply to digital products from non-EU manufacturers once they are placed on the EU market, the CRA would impact cybersecurity standards for such products beyond the EU's borders. As earlier mentioned, non-EU operators striving for efficiency might follow the CRA's rules as a default framework for their global operations – thus fueling the "Brussels effect" in an important manner and establishing the EU as the global standard-setter for the cybersecurity of connected devices.[155]

II. Risk-based classification of products

As seen before, the CRA covers a broad range of products. However, based on their level of risk, the CRA splits these products in two main categories: (1) default non-critical products, i.e., hardware and software with a low level of criticality[156] and (2) "critical products". The latter are products listed in Annex III, as well as products that have the core functionality of a category that is listed in Annex III.[157] Reflecting their inherent level of cybersecurity risk, the critical products are then divided into class I and class II as set out in Annex III.[158] This risk-based approach is typical for many of the CRA's rules but is certainly not unique to it.[159] It has indeed become a feature of EU's regulation

154 Cf. Sections C.III.2. and C.III.3 below for further clarification.

155 Car/De Luca (fn 14), 6; Bertuzzi Luca, Commission Expects to Set the World's Cybersecurity Standards for Connected Devices, EURACTIV.com, 27 September 2022, <https://www.euractiv.com/section/cybersecurity/news/commission-expects-to-set-the-worlds-cybersecurity-standards-for-connected-devices/> (cit.: Bertuzzi, September 2022).

156 Car/De Luca (fn 14), 6.

157 Art. 6(1) CRA Proposal.

158 Art. 6(1) CRA Proposal.

159 Chiara, Cyber Resilience Act (fn 8), 259.

of new technologies and is prominently showcased by the GDPR,[160] as well as by recent legislative developments, such as the proposed AI Act and the 2022 Digital Services Act (DSA).[161]

Following the risk-based approach, manufacturers must assess the cybersecurity risks associated with a product category and take this into account during the planning, design, development, manufacturing, distribution and maintenance of the product with digital elements.[162] While all products, regardless of their classification, must meet the essential cybersecurity requirements of Annex I, depending on their classification, products are subject to different conformity assessment procedures,[163] as we show below.

The EU estimates that the vast majority of products with digital elements (90%) will fall into the "default" category and only 10% are going to be classified as "critical".[164] The "default" category contains products such as photo-editing software, video games, smart speakers and hard drives.[165] Pursuant to Annex III, critical "class I" products with digital elements are password managers, network interfaces, firewalls, and microcontrollers.[166] Highly critical products, i.e., critical "class II" products are among others operating systems for servers, desktops and mobile devices, smart meters, CPUs and robot controllers.[167]

Annex III is however not conceived as an exhaustive list. Rather, the European Commission is empowered to adopt delegated acts to amend it,[168] and so

---

160 De Gregorio Giovanni/Dunn Pietro, The European Risk-based Approaches: Connecting Constitutional Dots in the Digital Age, Common Market Law Review 2022, 476.

161 Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act), OJ (2022) L 277/1 [hereinafter DSA]. However, those regulations differ in their approach towards risk regulation; De Gregorio/Dunn (fn 160), 477.

162 Chiara, Cyber Resilience Act (fn 8), 261.

163 Chiara, Cyber Resilience Act (fn 8), 260.

164 European Commission, Directorate-General for Communications Networks, Content and Technology, Cyber Resilience Act: New EU Cybersecurity Rules Ensure More Secure Hardware and Software Products, September 2022, <https://data.europa.eu/doi/10.2759/543836>.

165 European Commission, Directorate-General for Communications Networks, Content and Technology (fn 164).

166 Annex III of the CRA Proposal; cf. European Commission, Directorate-General for Communications Networks, Content and Technology (fn 164).

167 Annex III of the CRA Proposal; European Commission, Directorate-General for Communications Networks, Content and Technology (fn 164).

168 Art. 6(2) CRA Proposal.

if needed, take into account technical innovations. In view of the rapid technological developments and the related possibility that the risks of the products may change, the list will probably need to be continuously re-viewed.[169] However, it is doubtful whether the proposed review process can accommodate all developments. Already now the list of Annex III seems somewhat incomplete, given that tangible and intangible products with digital elements that perform cryptographic operations are not listed, while such products are of importance for effective information security, cybersecurity, data protection and privacy, and might be exposed to attacks.[170]

Another critical issue with the listing of Annex III is that it is unclear which criteria the Commission applied to identify and classify the listed products.[171] This could change insofar as Art. 6(3) CRA indicates that the Commission shall specify the characteristics of the product categories listed in Annex III in a delegated act to provide operators with guidance on how to determine with certainty whether and how their products are to be classified. Moreover, Recital 25 and Art. 6(2) CRA provide some criteria for determining if a product with digital elements is to be deemed "critical". Pursuant to Recital 25 "[p]roducts with digital elements should be considered critical if the negative impact of the exploitation of potential cybersecurity vulnerabilities in the product can be severe due to, amongst others, the cybersecurity-related functionality, or the intended use." Accordingly, one criterion for assessing the level of the cybersecurity risk of a product is whether it runs with privilege, privileged access, or performs a function critical to trust,[172] as such attributes can lead to a propagation of security issues throughout the supply chain.[173] Further criteria are the intended use in sensitive environments such as in industrial settings[174] or the intended use for the processing of personal data,[175] as well as the potential impact of an incident, in particular its ability to affect a large number of people.[176] That last criterion seems to be linked to the market share of a product. But this again runs the danger that products that are

169 Cf. Brass Irina/Sowell Jesse H., Adaptive Governance for the Internet of Things: Coping with Emerging Security Risks, Regulation & Governance 2021, 1102.

170 Cf. European Data Protection Supervisor (fn 105), 7.

171 Cf. TÜV Verband, Position Paper on the EU Commission Proposal for a Cyber Resilience Act, December 2022, <https://www.tuev-verband.de/index.php?eID=dumpFile&t=f&f=2933&token=b28683b4eaf5f0c41236b49c3373ea6852eaa17d>, 4.

172 Art 6(2) point a) CRA Proposal.

173 Recital 25 CRA Proposal.

174 Explanatory Memorandum to the CRA Proposal, 9 et seq.

175 Art. 6(2) point c) CRA Proposal.

176 Art. 6(2) point d) CRA Proposal.

not bestsellers would be deemed to be less risky merely because they have a smaller market share and therefore lesser ability to affect many people in case of an incident.

It is furthermore noteworthy that most of the criteria seem to mainly focus on the industrial side.[177] The classification in Annex III, respectively the classification of certain products as "non-critical" appears to indicate that the Commission deems industrial IoT more critical than consumer IoT, such as for instance smart speakers. This approach, however, may underestimate the fact that certain products should be treated as riskier since they are used to keep the user safe in the physical world, such as smart homes and security alarms, may process privacy-relevant data and/or are used by children.[178] Also, as the CRA classifies categories of products, it may unduly disregard the "operational environment" in which a product will be placed, even though threats and related risks of products can be extremely different depending on where they are used.[179] For instance, smart LED bulbs would likely be classified as non-critical products. However, if a smart LED light bulb is compromised, it can serve as a gateway into the network it is connected to and the threat can spread to an entire network.[180] If a smart LED bulb is used in a private home network, the ramifications of its compromise may be less problematic. However, if such a light bulb is in use in a factory and can thus be exploited as an entry point into the factory's network and for example be used to shut down the factory's production, the consequences could be much more widespread. Yet, this can also be the case in reverse, in particular in that industrial components are used for non-critical purposes.[181] Consequently, it is questionable if the "list-based" approach of Annex III is sufficiently robust to reflect the risks posed by products with digital elements under different circumstances.

---

177 Cf. Euroconsumers, EU Cyber Resilience Act: Will the Hackable Home Finally Be Secured?, September 2022, <https://www.euroconsumers.org/activities/cyber-resilience-act-will-hackable-home-be-secured>.

178 TÜV Verband (fn 171), 5; Bertuzzi, September 2022 (fn 155).

179 Cf. Digitaleurope (fn 135), 6.

180 Cf. Interagency International Cybersecurity Standardization Working Group (IICS WG), Interagency Report on the Status of International Cybersecurity Standardization for the Internet of Things (IoT), November 2018, <https://csrc.nist.gov/publications/detail/nistir/8200/fina>, 13 et seq.; cf. Johnson et al. (fn 7), 721.

181 Cf. VDMA, Uniform Cybersecurity Requirements Are the Only Right Way Forward, September 2022, <https://www.vdma.org/viewer/-/v2article/render/67648803>; ZVEI Germany's Electro and Digital Industry, Cyber Resilience Act: Important Step for More Cyber Security, September 2022, <https://www.zvei.org/en/press-media/pressarea/cyber-resilience-act-important-step-for-more-cyber-security>.

Some of the above points of critique appear to be addressed by a recently shared new compromise text of the Swedish presidency of the EU Council of Ministers. It is reported that this compromise comes with significant changes on the classification of critical and highly critical products and sheds some light on why and which products qualify as critical class I or class II products. Furthermore, the list of products was revised in that, inter alia, class I and class II products were divided into subgroups and consumer products such as smart locks and alarm systems were included.[182]

III. Obligations of economic operators along the supply chain and throughout the life-cycle of products

As noted earlier, the addressees of the CRA are the economic operators, in particular manufacturers, importers and distributors of products with digital elements.[183] These economic operators – depending on their role and responsibility within the supply chain – have to fulfil several obligations before and during the placing on the market of a product.[184] As the next sections show, there is a sliding scale of regulatory burden, starting with manufacturers at the top towards distributors at the scale's bottom.

1. Extensive obligations of manufacturers

A large number of obligations of the CRA are imposed primarily on manufacturers. This can arguably be based on the assumption that manufacturers form the beginning of the supply chain, thus having usually the most influence on the conception, design and development of their products.[185]

First of all, it is the obligation of the manufacturer to ensure that, when placing a product with digital elements on the market, it has been designed, developed and produced in accordance with the essential requirements set out in Section 1 of Annex I.[186] Those include the obligation to design, develop and produce products with digital elements in such a way that they ensure an appropriate level of cybersecurity based on their risks. Furthermore, they should not be delivered with known exploitable vulnerabilities, must be

182 Bertuzzi Luca, EU Council Reconsiders Critical Products in New Cybersecurity Law, EURACTIV.com, 15 February 2023, <https://www.euractiv.com/section/cybersecurity/news/eu-council-reconsiders-critical-products-in-new-cybersecurity-law/>.

183 Section C.I.4.

184 Car/De Luca (fn 14), 7.

185 Zirnstein (fn 145), 710.

186 Art. 10(1) CRA Proposal.

delivered with a secure by default configuration, must protect the confidentiality and integrity of the data they process and only process data, personal or other, that are strictly necessary to the functioning of the product.[187] Yet again, the list in Section 1 of Annex I is not to be understood as exhaustive.[188] While the manufacturers have to comply with all essential requirements related to vulnerability handling and have to ensure that they deliver their products without any known exploitable vulnerability, with respect to the other essential requirements manufacturers have to determine themselves which of them are relevant for the respective type of product.[189] In this sense, manufacturers must take a holistic view of whether the implementation of these requirements alone leads to an appropriate level of cybersecurity of their product or if they have to take additional case-specific measures.[190] This is reminiscent of Art. 32 GDPR in the context of personal data protection that also sets out a non-exhaustive list of security measures to ensure a level of security appropriate to the risk.[191]

Next to requirements that the products be designed, developed, and produced in such a way that they ensure an appropriate level of cybersecurity, the CRA follows the principle of security by design and makes it mandatory.[192] The basic idea behind security by design is that products should be designed with threats to security in mind and that vulnerabilities should be adequately addressed throughout a product's life-cycle.[193] In other words, products should be secure right from the moment they are made available, and they should be secure during their operational phase and remain secure during and after maintenance operations, such as updates. Moreover, once the product has reached its end-of-life, its secure disposal or recycling, especially the

---

187 European Economic and Social Committee (fn 23), 2; Car/De Luca (fn 14), 7.

188 Zirnstein (fn 145), 710.

189 Recital 32 CRA Proposal.

190 Zirnstein Yannick/Lee Yue Lin/Ge Amanda, Evolving Cybersecurity Landscape – Comparing the Regulatory Approaches in the EU, in China and in Singapore — An Analysis of Legislative Approaches to Key Issues in Tackling a Global Phenomenon, Computer Law Review International 2022, 167.

191 Cf. Haber Eldar/Tamò-Larrieux Aurelia, Privacy and Security by Design: Comparing the EU and Israeli Approaches to Embedding Privacy and Security, Computer Law & Security Review 2020, 4.

192 Section 1 (3a) of Annex I of the CRA Proposal. Schmitz-Berndt/Cole (fn 58), 11; cf. Car/De Luca (fn 14), 7.

193 Center for Security Studies, Governance Approaches to the Security of Digital Products - A Comparative Analysis, November 2021, <https://genevadialogue.ch/wp-content/uploads/Governance-Approaches-to-the-Security-of-Digital-Products-Report-2021-Geneva-Dialogue-and-EHTZ-CSS.pdf>, 19.

deletion of personal data that it contains, must be provided.[194] The security-by-design model is not new to cybersecurity, as it first emerged from computer engineering principles and was later proposed as a way to mitigate the security vulnerabilities presented by the IoT.[195] Since then, it has been reflected in cybersecurity law,[196] for instance in the NIS Directive and its update, in the Cybersecurity Act as well as in newer EU data governance legislation, such as the proposed AI Act and the Data Act.[197] In light of these similarities in approach, the EDPS has sought to interface the GDPR with the CRA and strongly recommends including data protection by design and by default in the essential cybersecurity requirements for products with digital elements.[198]

While the security-by-design approach set out in Annex I Section 1 is to be welcomed,[199] the requirement that "products with digital elements shall be delivered without any known exploitable vulnerability" might be over-ambitious, considering that for example the vulnerability in Log4j, the case discussed earlier, existed since 2013 and remained unnoticed until the end of 2021, even though Log4j has been highly popular and with widespread use. Ellul et al. argue that software-based products and services are inherently delivered with vulnerabilities, despite the increasing capabilities and ongoing development of technical assurances. This has to do with the common practice of ensuring that no software is released without undergoing testing – that is, the process of evaluating and validating software by running it in a controlled environment. While this practice seems relatively straightforward, the actual process is not. According to Ellul et al. it is not always easy to know what constitutes an appropriate test, and whether a test suite adequately captures the possible behaviour of the system. In addition, it is difficult to simulate the environment in which the system will operate during a test, especially in environments with malicious actors.[200] In this context, it appears that the initial text of the CRA is now being adapted in that the obligation not to place products with known exploitable vulnerabilities on the EU internal

194 van der Schaaf Koen/Tekinerdogan Bedir/Catal Cagatay, A Feature-based Approach for Guiding the Selection of Internet of Things Cybersecurity Standards Using Text Mining, Concurrency and Computation: Practice and Experience 2021, 7 et seq.

195 Bygrave Lee A., Security by Design: Aspirations and Realities in a Regulatory Context, Oslo Law Review 2021 (cit.: Bygrave, Security by Design), 126.

196 Bygrave, Security by Design (fn 195), 137 et seq.

197 Bygrave, Security by Design (fn 195), 138.

198 European Data Protection Supervisor (fn 105), 7.

199 European Data Protection Supervisor (fn 105), 2.

200 Ellul Joshua et al., When Is Good Enough Good Enough? On Software Assurances, ERA Forum 2023.

market will depend on the manufacturer's risk assessment. This means that if manufacturers assess the risk of a vulnerability as very low, the product can still be marketed. This amendment is intended to reduce bureaucracy and take into account cases in which a vulnerability can later be fixed by a security update.[201]

Another obligation towards manufacturers, given the emphasis put on the supply chain security, is the due diligence obligation, when manufacturers source third-party components for their products with digital elements and need to ensure that such components do not compromise the product's cybersecurity.[202] Furthermore, in order to ascertain and demonstrate compliance of their product with the essential cybersecurity requirements, manufacturers are required to undertake an assessment of the cybersecurity risks associated with a product with digital elements.[203] The CRA provides via Chapters III and IV and Annex VI for a rather extensive guidance on the conformity assessment, especially with respect to the procedure as well as on the conformity assessment bodies. Three aspects should be pointed out here: First, under certain conditions, there is a presumption of conformity for products with digital elements and processes put in place by the manufacturer.[204] This is the case, for instance, where European harmonization standards already exist for a particular area[205] and the product in question complies with these standards.[206] A second aspect worth highlighting is the fact that a manufacturer's choice for a conformity assessment procedure set out in Annex VI depends on the risk classification of his product.[207] For non-

---

201 Bertuzzi, February 2023 (fn 16).

202 Tuninetti Ferrari et al. (fn 151), 3; cf. Chiara, IoT (fn 63), 129.

203 Art. 10(2) CRA Proposal. However, under certain conditions, manufacturers are permitted under Recital 20 and Art. 4(3) CRA to release software for testing purposes before subjecting their product to a conformity assessment. Further on this as well as on the research and development indications of the CRA: Rosal Santos Isabela, Horizontal Cybersecurity Requirements: What Does the New European Proposal for Products with Digital Elements Add to R&D?, KU Leuven CiTiP Blog, 17 January 2023, <https://www.law.kuleuven.be/citip/blog/horizontal-cybersecurity-requirements-what-does-the-new-european-proposal-for-products-with-digital-elements-add-to-rd/>.

204 Cf. Art. 18 CRA Proposal.

205 Further on European cybersecurity certification schemes under the Cybersecurity Act: Kamara Irene, Misaligned Union Laws? A Comparative Analysis of Certification in the Cybersecurity Act and the General Data Protection Regulation, in: Hallinan Dara/Leenes Ronald/De Hert Paul (eds.), Privacy and Data Protection: Artificial Intelligence, Oxford 2020.

206 Art. 18(1) CRA Proposal.

207 Chiara, Cyber Resilience Act (fn 8), 260.

critical products, manufacturers can exercise a self-assessment, declaring that their products satisfy the essential security requirements of Annex I.[208] Manufacturers of critical product of class I and II however have to demonstrate conformity through an EU-type examination[209] or by full quality assurance[210], the latter involving a third-party.[211] In this sense, the risk-based approach in the product classification is also clearly reflected here. Considering that estimated 90% of the products with digital elements are likely to be classified as non-critical and will not trigger an external assessment, but a self-assessment by manufacturers,[212] this raises some doubts as to whether an adequate level of cybersecurity and a consistently high level of protection in a rapidly changing cybersecurity threat environment would be ensured.[213] And finally, the manufacturer has to provide a declaration of conformity according to Art. 20 CRA and digital products demonstrating compliance must be properly CE marked and may only be placed on the market with such marking.[214] Once a product receives a CE marking, it can be deployed in and move freely within the internal EU market,[215] thus fostering the functioning of the single market for products with digital elements.[216]

Manufacturers have also several documentation obligations. Following Art. 23 they need to draw up a comprehensive technical documentation before the product is placed on the market,[217] with the minimum requirements for this documentation specified in Annex V. Furthermore Art. 10(10) CRA obliges manufacturers to ensure that products are accompanied by the information and instructions set out in Annex II. The information should be provided in an electronic or physical form and the language should be clear, understandable, intelligible and legible.

---

208 Car/De Luca (fn 14), 7 et seq.

209 Annex VI, Module B CRA Proposal.

210 Annex VI, Module H CRA Proposal.

211 Explanatory Memorandum to the CRA Proposal, 10 et seq.; Car/De Luca (fn 14), 7 et seq.

212 TIC Council, TIC Council Welcomes the European Commission's Proposal for a Cyber Resilience Act, September 2022, <https://www.tic-council.org/news-and-events/news/press-release-tic-council-welcomes-european-commissions-proposal-cyber-resilience-act>; Euroconsumers, (fn 177).

213 TÜV Verband (fn 171), 4.

214 Arts. 21 and 22 CRA Proposal.

215 Art. 4(1) CRA Proposal.

216 Zußner (fn 149), 194.

217 Chiara, Cyber Resilience Act (fn 8), 261.

Article 10(6) CRA imposes further the obligation on manufacturers, upon placing a product with digital elements on the market, to ensure that vulnerabilities of that product are addressed effectively and in accordance with the essential requirements of Section 2 of Annex I of the CRA during the expected lifetime of the product or during a period of five years from the date on which the product is placed on the market, whichever is shorter. Consequently, during the maximal period of five years manufacturers have to continuously test whether their products still comply with the legal requirements and if this is not the case, they must take all necessary measures to restore compliance.[218]

One finds no explanation in the CRA why the period of five years was chosen.[219] Considering the fact that many products have a longer lifetime, this period may be inadequate, especially since the EU strives for sustainability of products.[220] If products no longer receive security updates after the five years have expired, they can easily turn into a dangerous gateway for attacks.[221] There is a related concern also for products that are already on the market for some time and the five year period has almost expired – let us say after four and half years on the market. Although in this example the user would still benefit from security updates for six months, he may continue to use the product for years afterwards without further receiving security updates. While admittedly, users are provided with the information on the period up to which the manufacturer offers security support as per the information obligations of Art. 10(10) in connection with Annex II, this does not change the potential risk situation for the product, especially as used products can easily be resold on existing auction and other platforms.

These concerns fortunately appear to be addressed in a subsequently agreed upon amendment of the CRA proposal. It is reported that the compromise will be amended in that manufacturers shall ensure the security of their products "for a period of time after the placing on the market, appropriate to the type

218 Zirnstein (fn 145), 710.

219 Cf. Kipker (fn 137).

220 Inter alia EU's New Consumer Agenda (Communication from the Commission to the European Parliament and the Council, New Consumer Agenda, COM(2020) 696 final, 13 November 2020) and the Circular Economy Action Plan (Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A New Circular Economy Action Plan, COM(2020) 98 final, 11 March 2020) aim at promoting repair and encouraging more sustainable products.

221 Zirnstein (fn 145), 710 et seq.; cf. Euroconsumers (fn 177).

of product and its expected lifetime."[222] This adequately takes into account now that each product has a different life-cycle, which the manufacturer has to assess himself, based on the time that users reasonably expect to receive security updates, considering the functionality and the intended use of the product. Further, the manufacturer has a duty of care to provide security updates for at least 10 years. The same period applies if the manufacturer becomes aware or has reason to believe that his product no longer complies with the security requirements of the CRA.[223]

Still, there is a concern as to how the end of the update obligation is to be assessed in light of the idea of security by design, which entails a life-cycle approach. The CRA seems to follow this life-cycle approach for most parts as Art. 10(1) demands products to be designed, developed and produced in accordance with the essential cybersecurity requirements and Art. 10(6) lays down essential requirements for vulnerability handling. Apart from the above noted dilemmas around a product's operation phase and the associated with it obligations, at some point, the product will reach its end of lifespan. Yet, one finds no security requirements in the CRA that would address how to ensure products' cybersecurity at the end of its life-cycle. The secure disposal of a device, especially the secure removal of information in the device, is at the same time absolutely key.[224] Information erasing is also elemental where the device is not completely decommissioned but reused or refurbished.[225] Furthermore, the big question looms of how all these obligations are to be realized in practice.[226] In reality, it is common that the manufacturer does not know the end user because the product with digital elements is not sold directly by the manufacturer but through distributors, or the product has been resold.

Finally, manufacturers carry certain reporting obligations. Pursuant to Art. 11 CRA, the manufacturer must report any actively exploited vulnerability of a product with digital elements and any incident affecting its security to ENISA without delay, but within 24 hours of becoming aware of them. The

---

222 Bertuzzi, February 2023 (fn 16).

223 Bertuzzi, February 2023 (fn 16).

224 European Union Agency for Cybersecurity, Guidelines for Securing the Internet of Things, Secure Supply Chain for IoT, November 2020, <https://www.enisa.europa.eu/publications/guidelines-for-securing-the-internet-of-things/@@download/fullReport>, 12; van der Schaaf/Tekinerdogan/Catal (fn 194), 7 et seq.

225 European Union Agency for Cybersecurity (fn 224), 12.

226 Cf. Nai Fovino Igor et al., Cybersecurity, Our Digital Anchor, June 2020, <https://publications.jrc.ec.europa.eu/repository/bitstream/JRC121051/cybersecurity_online.pdf>, 90.

manufacturer must also notify without delay the users of the product, irrespective of the risk, and inform them of corrective measures they can take.[227] Here, the CRA seems to diverge from the GDPR, which, based on its risk-based approach, requires data breach notification of users, respectively data subjects, only if the breach is likely to result in a high risk to the rights and freedoms of natural persons.[228] Also the NIS2 Directive only requires a notification to users in case of "significant incidents that are likely to adversely affect the provision of the services" of the entities.[229]

While swift reporting of incidents seems sensible, given that security incidents can spread within minutes, the formulation "any incident" in Art. 11(2) CRA can be understood as that every vulnerability, even if it poses no noticeable impact on the security of a product, triggers the reporting obligation of the manufacturer. Furthermore, the CRA reporting obligations are not aligned with processes that are already in place – for instance, the timeframe of 24 hours differs from the 72 hours given under the GDPR and the NIS2 Directive.[230]

As with previous concerns, these seem to be recognized and there is an effort to tackle them. A newly reached compromise strives in this sense to align the CRA reporting obligation with the NIS2 Directive, shifting also the reporting from ENISA to the national Computer Security Incident Response Team (CSIRT).[231]

2. Importers as watchdogs

While importers themselves are not responsible for ensuring that products meet the essential cybersecurity requirements set out in Section 1 of Annex I, they are not permitted to import products into the European market that do not meet the respective requirements.[232] In case an importer considers or has reason to believe that a product is non-compliant, he should refrain from placing the product on the market until it has been brought into conformity by the manufacturer.[233] Consequently, in order to avoid infringing their own obligations, it will be imperative for importers to carry out a full inspection

227 Art. 11(1) and (2) CRA Proposal.

228 Cf. Haber/Tamò-Larrieux (fn 191), 4.

229 Art. 23(1) NIS2 Directive.

230 Art. 32(1) GDPR; Art. 23(4) NIS2 Directive.

231 Bertuzzi, February 2023 (fn 16).

232 Art. 13(1) CRA Proposal.

233 Art. 13(3) CRA Proposal.

of every product that they wish to import,[234] although Art. 13(2) CRA only obliges them to ensure that the manufacturer has carried out the appropriate conformity assessment procedures and has drawn up the technical documentation. Furthermore, they have to check that the product bears the CE marking and is accompanied by the instructions and information set out in Annex II.

By imposing such obligations on the importer, in particular to verify that the manufacturer is complying with his obligations under Section I of Annex I, Art. 13 assigns a "watchdog" function to the importer vis-à-vis the manufacturer. This role is also observable in Art. 13(6) CRA, which obliges the importer to support manufacturers in their vulnerability management and inform the manufacturer immediately if they become aware of a vulnerability. In addition, if the respective product poses a significant cybersecurity risk from the importer's perspective, importers must also inform the market surveillance authority.[235] Apart from this "watchdog" role, importers carry certain transparency related duties and must provide their contact details in the way specified in Art. 13(4) CRA.

3. Few duties for distributors

Unlike the importer, the distributor does not have to verify whether a manufacturer's products comply with the essential cybersecurity requirements. Before making the product available on the market, the distributor only has to check whether the product bears the CE marking and whether the manufacturer and the importer have complied with the obligations set out respectively in Arts. 10(10), 10(11) and 13(4)[236] – that is, whether the manufacturer has provided the required information according to Annex II as well as the declaration of conformity and, in the case of the importer, whether the name and contact information are provided.

These "light" obligations of the distributor, compared to the ones of the manufacturer and importer, can be explained by the fact that the distributor forms the end of the supply chain and as such has no relevant influence on the development, manufacturing and upstream distribution process.[237] Still, the distributor seems to be assigned also with some watchdog functions in that, like the importer, the distributor may not (or no longer) place a product on the market in case he believes or has reason to believe that a product is not in

234 Zirnstein (fn 145), 711.

235 Art. 13(3) CRA Proposal.

236 Art. 14(2) CRA Proposal.

237 Zirnstein (fn 145), 711.

conformity with the essential cybersecurity requirements.[238] The distributor must also inform the manufacturer, as well as the market surveillance authority, if a products poses a significant cybersecurity risk.[239]

IV. Comprehensive market surveillance and enforcement mechanisms

The CRA grants the European Commission, ENISA as well as national market surveillance authorities comprehensive market surveillance, investigation and ordering competences. Market surveillance for products with digital elements was already introduced with Regulation (EU) 2019/1020[240] on market surveillance and compliance of products by relevant authorities.[241] Member States may designate one or more existing authorities as market surveillance authorities or establish new ones.[242] However, for products with digital elements under the CRA that are classified as high-risk AI systems according to the AI Act, it is the market surveillance authorities pursuant to the AI Act that are responsible.[243]

Market surveillance authorities carry out market surveillance in the territory of the respective Member State. As far as necessary, they must be in constant exchange with their counterparts in other Member States as well as with data protection supervisory authorities.[244] In contrast to the GDPR and the Digital Services Act, the CRA does not create a one-stop-shop mechanism to address cross-border infringements.[245] It does, however, aim to establish a dedicated administrative cooperation group (ADCO) to ensure CRA's uniform application.[246] This ADCO is to be composed of representatives of the market surveillance authorities and representatives of single liaison offices.[247]

---

238 Art. 14(3) CRA Proposal; cf. Tuninetti Ferrari et al. (fn 151), 5 et seq.

239 Art. 14(3) CRA Proposal.

240 Regulation (EU) 2019/1020 of the European Parliament and of the Council of 20 June 2019 on market surveillance and compliance of products and amending Directive 2004/42/EC and Regulations (EC) No 765/2008 and (EU) No 305/2011, OJ (2019) L 169/1.

241 Explanatory Memorandum to the CRA Proposal, 11.

242 Art. 41(2) CRA Proposal.

243 Art. 41(10) CRA Proposal.

244 Art. 41(4) and (5) CRA Proposal.

245 Tuninetti Ferrari et al. (fn 151), 6.

246 Recital 56 CRA Proposal.

247 Art. 41(11) CRA Proposal.

The purpose of the national market surveillance authorities is to ensure the effective implementation of the CRA.[248] In order to do so they may initiate investigations following Art. 43 if they have sufficient reason to consider that a product with digital elements presents a significant cybersecurity risk.[249] To be able to evaluate the conformity of products, the authority shall be granted access to the data that it needs to assess the design, development, production and vulnerability handling, including also related internal documentation.[250] Where the market surveillance authority reaches the conclusion that the product does not comply with the requirements of the CRA, it may, commensurate with the nature of the risk, order the relevant operator to take all necessary measures to make the product compliant, to withdraw it from the market or to recall it.[251] If the operator does not take the corrective actions within the given timeframe, the authority shall take the appropriate measure.[252]

In case the Commission has reasons to consider that a product with digital elements is non-compliant with the CRA, the Commission can request the respective national market surveillance authority to carry out an evaluation according to Art. 43.[253] However, it is also possible that the Commission requests ENISA to carry out an evaluation of compliance.[254] This is the case where the exceptional circumstances justify an immediate intervention, there is sufficient reason to consider that the product remains non-compliant, and no effective measures have been taken by the relevant market surveillance authority.[255] Pursuant to Recital 59 CRA, an "exceptional circumstance" is present, for instance where a non-compliant product is made available throughout several Member States, used also in key sectors, and contains known and already exploited vulnerabilities for which the manufacturer does not provide patches. The Commission may intervene, based on ENISA's evaluation, by adopting implementing acts to decide on measures at the Union level, which may include ordering the withdrawal of the product or recalling it.[256]

---

248 Art. 41(2) CRA Proposal.

249 Zirnstein/Lee/Ge (fn 190), 170.

250 Art. 42 CRA Proposal.

251 Art. 43(1), (4) and (5) CRA Proposal.

252 Chiara, Cyber Resilience Act (fn 8), 265.

253 Art. 45(1) CRA Proposal.

254 Chiara, Cyber Resilience Act (fn 8), 265.

255 Art. 45(2) CRA Proposal.

256 Art. 45(3) and (4) CRA Proposal.

Even where products comply with the CRA, market surveillance authorities have the power to intervene via Art. 46. The prerequisite for this is that the product poses a significant cybersecurity risk despite its compliance with the cybersecurity requirements and the product furthermore poses a risk to particular rights or goods,[257] such as the health or safety of persons, compliance risks in relation to fundamental rights or other aspects of the protection of public interests.[258] The criterion "other aspects of the protection of public interests", however, seems rather broad and vague given the fact that if the prerequisites are met, Art. 46(1) provides the market surveillance authority to take the same measures as the authority has in case of non-compliant products, i.e., the authority might even demand the recall of compliant products.[259] It is also with regard to compliant products, where the Commission is provided with the possibility to intervene and establish corrective or restrictive measures, similarly to those under Art. 45 concerning the EU-level procedure for products with digital elements presenting a significant cybersecurity risk.[260]

Apart from these intervention possibilities, following Art. 48 CRA several market surveillance authorities can also agree to carry out joint activities to verify compliance and identify cybersecurity risks of products with digital elements that are often found to present such risks.[261] Joint activities might also be proposed by the Commission or ENISA.[262] Particularly drastic joint activities are the so-called "sweeps".[263] These are simultaneous coordinated control actions of certain products or categories thereof in order to check their compliance with the CRA.[264] In other words, market surveillance authorities can simulate area-wide and cross-border cyberattacks on products that are already on the market and in use.[265] According to Recital 61 CRA, sweeps should particularly be conducted "where market trends, consumer complaints or other indications suggest that certain product categories are often found to present cybersecurity risks." Given that sweeps are an intensive intervention with respect to the rights and freedoms of market participants and users, it can be noted that these criteria are again

257 Zirnstein/Lee/Ge (fn 190), 170.
258 Art. 46(1) CRA Proposal.
259 Art. 46(1) CRA Proposal.
260 Cf. Art. 48(6 et seqq.) CRA Proposal.
261 Cf. Recital 60 CRA Proposal.
262 Art. 48(2) CRA Proposal.
263 Zirnstein (fn 145), 713.
264 Art. 49(1) CRA Proposal.
265 Zirnstein (fn 145), 713.

somewhat broad and vague.[266] If clearer criteria not only on the deployment but also on the process of such control actions can be established, such sweeps can be a viable way to verify that a product is secure in practice.[267]

Overall, the monitoring and oversight over the compliance with the CRA is considerable and complex.[268] This can be in practice linked to problems of coordination between the different national authorities.[269] There is also a risk of fragmentation of surveillance resulting from the unclear wording in Art. 43(1), which states that a market surveillance authority may initiate investigations if it considers a product to present a "significant cybersecurity risk". Consequently Art. 43(1) leaves it to the discretion of the market surveillance authority which products are to be investigated or not. This may result in inconsistent procedures within the EU.[270] Asymmetry between national market surveillance authorities may also unfold as a result of different set of resources and institutions that an authority may use. In this sense, the varying levels of cybersecurity preparedness among Member States may present an obstacle to harmonization, mutual recognition, and convergence.[271] Accordingly, the requirement in Art. 41(6) CRA, whereby Member States must provide adequate resources, is particularly important and ultimately critical for the CRA's efficiency on the ground and throughout the Union.[272]

V. Significant administrative fines

The power to set rules on penalties is delegated to the Member States. Yet, the Member States' discretions are relative,[273] as Art. 53 already sets certain parameters. In general, all penalties imposed must be effective, proportionate and dissuasive.[274] More concretely: in case of a failure to comply with the essential requirements of Annex I and the obligations set out in Arts. 10 and 11 market surveillance authorities may impose fines of either €15 million or 2.5% of the total annual turnover of the previous business year, whichever is

266 Zirnstein (fn 145), 713.

267 Cf. Ludvigsen Kaspar Rosager/Nagaraja Shishir, The Opportunity to Regulate Cybersecurity in the EU (and the World): Recommendations for the Cybersecurity Resilience Act, <https://arxiv.org/abs/2205.13196>, 17.

268 European Economic and Social Committee (fn 23), 1.

269 European Economic and Social Committee (fn 23), 5.

270 Chiara, IoT (fn 63), 127 et seq.

271 Christou George, Cybersecurity in the European Union: Resilience and Adaptability in Governance Policy, London 2016, 177.

272 European Economic and Social Committee (fn 23), 1.

273 Chiara, Cyber Resilience Act (fn 8), 265.

274 Art. 53(1) CRA Proposal.

higher.[275] The bulk of risking fines is therefore borne by the manufacturer and other persons who are deemed to be manufacturers.[276] For non-compliance with other obligations of the CRA, market surveillance authorities can impose administrative fines of up to €10 million or 2% of global annual turnover for the previous fiscal year, whichever is higher.[277] This risk is borne by all economic operators – manufacturers, importers, as well as distributors.[278] For the supply of incorrect, incomplete or misleading information to market surveillance authorities in connection with an official investigation, a fine of €5 million or 1% of the total worldwide annual turnover for the previous fiscal year, whichever is higher, may be imposed.[279]

When deciding on the amount of the administrative fine in each individual case, the market surveillance authority should take into account all relevant circumstances of the specific situation and as a minimum the nature, gravity, duration and consequence of the infringement; whether other authorities have already imposed fines for similar infringements; and the size and market share of the operator.[280]

At a first glance, one may well conclude that the CRA follows the fines model of recent EU law, such as the GDPR as well as the proposed AI Act.[281] Yet, it remains to be seen whether the fines will amount to similar sums as those imposed under the GDPR and whether differences in the authorities' approaches to fines will also materialize in case of the CRA.[282] It should be borne in mind that, as shown above, the market surveillance authorities also have the option of banning products on the market, which can be an important tool of intervention. The interplay between these two mechanisms (fines vs. barring from the EU market) is so far not clarified in the CRA and may need additional attention before its final adoption.

D. Concluding observations and outlook

The article provided an enquiry into the EU proposal for a Cyber Resilience Act and attempted above all two things – on the one hand, to analyze more

275 Art. 53(3) CRA Proposal.
276 Zirnstein/Lee/Ge (fn 190), 170.
277 Art. 53(4) CRA Proposal.
278 Car/De Luca (fn 14), 8.
279 Art. 53(5) CRA Proposal.
280 Recital 65 and Art. 53(6) CRA Proposal.
281 Zirnstein/Lee/Ge (fn 190), 170.
282 Zirnstein/Lee/Ge (fn 190), 170; Ludvigsen/Nagaraja (fn 267), 11.

closely some of the key CRA provisions and on the other, to put the reform that the CRA will bring about into the broader context of EU's legal, policy as well as geopolitical activities in the digital domain in general and cybersecurity in particular. It is evident from the above that the CRA, when adopted, would cause a major stir and trigger a series of obligations for all actors engaged along the life-cycle of products with digital elements, create new competences for EU and Member State agencies and generate new interfaces with existing EU regulation in the domain of cybersecurity but also in other areas, such data protection and AI.

The ambitious regulatory project of the CRA and its potential far-reaching implications can be linked in general terms to its approach to cybersecurity as a cross-sectoral issue and the underlying conceptualization of cyber resilience as not merely a technical but a much wider topic of immediate societal relevance.[283] In more concrete terms, the regulatory sway of the CRA comes from its broad and comprehensive scope of application, the detailed catalogue of obligations (especially for manufactures of products with digital elements), as well as the potentially impactful market surveillance and enforcement mechanisms. Crucial for the effective approach of the CRA is also the inclusion of the entire value chain of digital products along their life-cycle, which is a new legal approach that duly takes into account both the dynamics of technological innovation as well as the premise of cyber resilience, whereby cyber threats are the rule rather than the exception.[284] While the CRA does take cyber resilience seriously, it also seeks to ensure that the single market for digital products is not unduly compromised and adopts a risk-based approach with varied regulatory burden across types of products and types of actors.

Despite the promise of the CRA and its regulatory potence, many questions remain still unanswered. These questions are of different nature and their answers will ultimately be quite different. Some of the definitional problems, lack of clarity and guidance in the CRA proposal, as well as the coordination problems with existing (and forthcoming) pieces of EU legislation can certainly be solved – either through compromises made during the still ongoing legislative process, through additional guidelines by the Commission or if somewhat less swiftly, through follow-up jurisprudence. There are however bigger questions and our contextualization of the CRA in the beginning of

283 Kipker (fn 137); Nai Fovino et al. (fn 226), 93; Bygrave Lee, Cyber Resilience versus Cybersecurity as Legal Aspiration, 14th International Conference on Cyber Conflict: Keep Moving 2022 (cit.: Bygrave, Cyber Resilience), 27.

284 Bygrave, Cyber Resilience (fn 284), 27.

the article speaks to them. The first important issue is whether the CRA, despite its virtues, could effectively lead to an Internet of Secure Things in Europe. Some of the concerns in this regard stem from endogenous to the CRA issues, such as that most digital products will be classified as low risk, the sliding scale of obligations, the possible divergences in surveillance practices and fines across responsible agencies. Others stem from even harder problems linked to the CRA's implementation in practice. In this context, it remains to be seen whether the CRA is adaptable enough to keep up with the rapidly evolving threat environment inherent to connected devices. Here one can consider for instance the fact that cybercriminals increasingly use malicious AI to support attacks, often to thwart intrusion detection algorithms within the IoT, or to attack beneficial AI in a way that causes the AI to work against its own system.[285] Also, given that the sophisticated AI application ChatGPT (with others to join it) can be used to proficiently write computer code, virtually anyone could exploit this to create their own malware to spy on user activity, steal data, spread ransomware or undertake any other malicious cyberattack.[286] Another big unknown in this dynamic context are users. While it appears that consumers would be willing to pay more for secure IoT devices,[287] the problem of informational asymmetry in the marketplace remains.[288] Similarly, the big question mark around user literacy and to what extent users are able and willing to react when faced with insecure digital products is unaddressed and may in reality reduce the CRA's efficacy despite the huge regulatory burden placed on the supply side. In this and the overall implementation context of the CRA, it would be particularly interesting, and potentially fruitful for policy makers, to observe and detect parallels with the implementation of the GDPR as another grand EU regulatory project.

Some of the critique points that can be expressed towards the CRA are of exogenous nature and can be linked to the CRA's underlying rationale to boost EU's role as a global cybersecurity standard-setter and a vector for safeguarding and sustaining its digital sovereignty – the second discrete topic that this article picked up at its outset. From the perspective of the Union, such a "digital sovereignty"-oriented strategy and the therewith related

---

285 Kuzlu Murat/Fair Corinne/Guler Ozgur, Role of Artificial Intelligence in the Internet of Things (IoT) Cybersecurity, Discover Internet of Things 2021.

286 Marr Bernard, How Dangerous Are ChatGPT and Natural Language Technology for Cybersecurity?, Forbes, 25 January 2023, <https://www.forbes.com/sites/bernardmarr/2023/01/25/how-dangerous-are-chatgpt-and-natural-language-technology-for-cybersecurity/?sh=52b374864aa6>.

287 Johnson et al. (fn 7), 721.

288 Johnson et al. (fn 7), 722.

regulatory activism in cybersecurity and beyond make lots of sense and can be easily politically justified. Yet, the EU, despite its sizeable market, is still part of the even larger landscape of the world and the datafication of economies and societies as a whole has only increased connectedness and interdependence between and across actors. After a period of relatively liberal stance towards cyberspace, in recent years and absent an international legal framework governing data, national legislators have adopted far-reaching rules on data protection, cybersecurity, competition, consumer protection, etc., often with an extra-territorial effect. It can be maintained that the EU has even been the regulatory champion in this regard. Yet, this leads to a profound fragmentation in the global data governance framework that we should be aware of.[289] Whether the "Brussels effect" of the CRA will unfold is still unknown but it too can contribute to exacerbating this fragmentation, as well as to increasing geopolitical tensions and strategic competition across different policy areas, which ultimately contribute little to a functioning, seamless data economy and a corresponding optimal legal design.[290]

Against this backdrop, it remains to be seen to what extent and how the CRA will manage to find its place in the complex puzzle and navigate the different trade-offs – such as between cybersecurity and market freedom, between protectionism and openness, between unilateral action and international cooperation.

---

289 Arner Douglas W./Castellano Giuliano G./Selga Eriks K., The Transnational Data Governance Problem, Berkeley Technology Law Journal 2023, 623.

290 Arner/Castellani/Selga (fn 290); also Aaronson Susan, What Are We Talking about When We Talk about Digital Protectionism?, World Trade Review 2018, 541; Bonefeld-Dahl Cecilia, European Sovereignty or a Shadow of Protectionism?, EURACTIV.com, 25 August 2022, <https://www.euractiv.com/section/digital/opinion/european-sovereignty-or-a-shadow-of-protectionism/>.