Review of European and Comparative Law | **2026**
Vol. 64, No. 1, 103–116
https://doi.org/10.31743/recl.19198
Received: 10 November 2025 | Accepted: 26 February 2026 | Published: 31 March 2026

The Concept of Cyber Resilience in the European Union Law

Grażyna Szpor

PhD habil., Professor, Department of Informatics Law, Faculty of Law and Administration, Cardinal Stefan Wyszyński University in Warsaw; correspondence address: Wóycickiego 1/3 Street, building 17, 01–938 Warsaw, Poland; e-mail: g.szpor@uksw.edu.pl
https://orcid.org/0000-0002-3264-9360

Abstract: The legal framework for digital transformation in the European Union is being supplemented by further acts that should enable it to meet current challenges while respecting EU values and principles redefined in the context of cyberspace. An example is Regulation 2024/2847 on horizontal cybersecurity requirements (Cyber Resilience Act). It does not define the term used in the abbreviated title. The relationship between cyber resilience and cybersecurity, and their place within the conceptual framework of digital transformation, remains unclear. This article aims to identify terminological issues that require doctrinal agreement, to consider the possibilities for achieving this, and to propose solutions. An analysis of how the purpose of the act is reflected in its title, definitions, scope, structure and initial stage of application was carried out using a legal-dogmatic method, including a systemic approach. It confirmed the verified hypotheses about the underestimation of the importance of short titles of acts in EU legislative processes and the untapped potential of the concept of cyber resilience in increasing the consistency and transparency of law, which is essential for its effectiveness. The result is a proposal to amend EU legislative drafting rules on short titles and to adopt a general definition of cyber resilience as a higher-order concept capable of integrating scattered sectoral regulations and performing an organizing function for digital transformation processes in legal doctrine.

Keywords: EU law, digital transformation, cybersecurity, cyber resilience, definition

1. Introduction

The role of law in digital transformation is to remove barriers to development, while also establishing restrictions deemed necessary to protect fundamental human rights and the public interest. Legal instruments for cybersecurity protection initially focused on incident response. However, due to the rapid increase in cyberattacks, including cyber operations conducted by hostile states, legislators have shifted their approach from reactive to proactive, encompassing broader diagnosis and threat reduction.[1]

In addition to changes in "sectoral" regulations, "horizontal" solutions have also emerged. An example is the Cyber Resilience Act (2024/2847)[2] (hereinafter: CRA), which

[1] Bolesław Szafrański, ed., *Cyberbezpieczeństwo: redefinicja zagrożeń* [Cybersecurity: Redefining Threats] (Warsaw: Wojskowa Akademia Techniczna, 2023).

[2] Regulation (EU) 2024/2847 of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) (OJ L, 2024/2847, 20 November 2024) (hereinafter: CRA).

ISSN 2545-384X (Online)

establishes horizontal cybersecurity requirements for products with digital elements.[3] The term "cyber resilience" has no legal definition, so its meaning needs to be verified.

Using a legal-dogmatic method, including systemic interpretation, the following parts of this article analyze: the compliance of the title of the regulation with EU legislative principles; the contexts in which the term cyber resilience appears (in the regulation and in other acts); the division of the protection of the cyber resilience of products with digital elements between the CRA and other acts; the links between the CRA glossary and the conceptual framework of digital transformation; the addressees of new obligations in the phase of partial application of the CRA.

In existing interdisciplinary research focusing on many aspects of cyber resilience, the meaning of this term is interpreted differently,[4] prompting attempts at harmonization. Assessments of legalization should also take into account the criteria of consistency and transparency, whose importance for the effectiveness of law is highlighted by new EU initiatives such as the Omnibus.[5]

2. Title and Purpose of the Cyber Resilience Act

The titles of EU legislative acts, including regulations, are determined by the Annex 1 of the *Joint Handbook for the Presentation and Drafting of Acts Subject to the Ordinary Legislative Procedure*,[6] adopted in October 2023 to facilitate cooperation between the European Parliament, the Council, and the Commission. It is not binding on the political bodies involved in the legislative process, but it does provide a "toolbox" that significantly impacts the formal aspects of new acts.

According to the guidelines contained in this document, the title of the act should signal its content in as concise and complete a manner as possible, without misleading the recipient as to the content of the normative part. The full title of the act may be followed by a short title. Therefore, the title Regulation (EU) 2024/2847 of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020, and Directive (EU) 2020/1828 (Cyber Resilience Act)[7] is generally in line with EU legislative drafting principles. However, it is not clear whether this also applies to the short title.

---

3 In addition, it amends two previous regulations: 168/2013 and 2019/1020, as well as Directive 2020/1828, and also contains a number of provisions referring to previously adopted EU acts.

4 Igor Linkov and Alexander Kott, "Fundamental Concepts of Cyber Resilience: Introduction and Overview," in *Cyber Resilience of Systems and Networks: Risk, Systems and Decisions*, eds. Alexander Kott and Igor Linkov (Cham: Springer, 2019), 1–25, https://doi.org/10.1007/978-3-319-77492-3_1.

5 European Commission, *Omnibus I*, COM(2025) 80 final (Brussels: European Commission, 26 February 2025); European Commission, *Omnibus II*, COM(2025) 84 final (Brussels: European Commission, 26 February 2025).

6 European Parliament, Council of the European Union, and European Commission, *Joint Handbook for the Presentation and Drafting of Acts Subject to the Ordinary Legislative Procedure*, October 2023 ed., Annex I: *Joint Practical Guide of the European Parliament, the Council and the Commission for Persons Involved in the Drafting of European Union Legislation*, pt. 8, pp. 18–20, https://www.consilium.europa.eu/media/67390/joint_handbook_en_01-october-2023_clean_def_final.pdf.

7 CRA (OJ L, 2024/2847, 20 November 2024).

The guidelines assume that short titles in Union law, where acts are identified by letters and numbers (e.g., (EU) 2025/1234), are less useful than in systems that do not use such a numbering system. It is emphasized that

> 8.4. In certain cases, however, a short title has come to be used in practice (…). Despite the fact that it may seem a simple solution, referring to acts by a short title creates risks for the accuracy and coherence of legal acts of the Union. This method should therefore only be used in specific cases where it significantly aids the reader's understanding.
>
> 8.5. The creation of a short title when an act is adopted by adding it after the title of the act should be avoided, since it only renders the title more cumbersome (…). While the risks outlined in point 8.4 must always be borne in mind, it is possible to refer to an act by using a short title in order to make it easier to understand the act in which the reference is made. In this case, the short title chosen will have to appear in brackets in the body of the text of the act in which the reference is made, like any other abbreviation.[8]

The main regulations and directives on digital transformation often have abbreviated titles.[9] At the same time, in scientific publications and public discourse, these abbreviated titles are widely used and sometimes replaced by even more informal abbreviations, mainly acronyms of elements of the title in English (NIS, CRA) or the national language. For example, in Poland, the commonly used term is not "General Data Protection Regulation" or GDPR,[10] but RODO. When applying the law, it is usually necessary to address the dispersion of many acts related to a specific administrative matter. The use of numbers makes the texts of the grounds for judgments and decisions incomprehensible to the recipient. This justifies the recommendation to amend the EU guidelines by abandoning the "uniqueness" of placing the abbreviated version of the title of a regulation or directive at the end.

A separate issue is the content of short titles and their placement in the provisions to which they refer. For example, in the CRA, the term "cyber resilience" appears in the title, in five recitals of the preamble and only once outside the preamble, in Article 33(2) (cyber resilience regulatory sandboxes). Recital (1), which states that cybersecurity is one of the most serious challenges facing the Union, seems to be of fundamental importance for the adoption of the short title:

> In the coming years, the number and variety of devices connected to the internet will grow rapidly. Cyberattacks are a matter of public interest because they have a decisive impact not only on the Union's economy, but also on the democratic system, consumer safety and health. It is therefore necessary to strengthen the Union's approach to cybersecurity, address the issue

---

8 European Parliament, Council of the European Union, and European Commission, *Joint Handbook for the Presentation and Drafting of Acts Subject to the Ordinary Legislative Procedure*, pts. 8.4–8.5, p. 19, https://www.consilium.europa.eu/media/67390/joint_handbook_en_01-october-2023_clean_def_final.pdf.

9 For example: Data Act, Data Governance Act, Digital Service Act, Artificial Intelligence Act, Interoperable Europe Act, Cybersecurity Act, Cybersolidarity Act. When considering the introduction of the prefix "cyber" into the titles of acts, it should be noted that in English, this prefix already appears in over 600 words.

10 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 L 119, 4 May 2016), 1–88.

of cyber resilience at Union level and improve the functioning of the internal market by establishing a single regulatory framework covering essential cybersecurity requirements for the placing of products with digital elements on the Union market.

The short titles of other EU acts refer to legally protected values such as security and solidarity, which are redefined in the context of cyberspace,[11] e.g., in the Cybersecurity Act[12] or the Cyber Solidarity Act.[13] This raises the question of whether the term "cyber resilience" used in the short title of Regulation 2024/2847, which refers to products with digital elements, can also be treated as a systemic category linking many regulatory regimes and, more broadly, whether the reference to protected values[14] should not be the first choice and become good practice in the formulation of short titles.

3. Definitions

The term "cyber resilience," which appears in the title of Regulation 2024/2847, has not yet been given a legal definition, nor does the CRA contain one. However, the lack of a legal definition does not mean that there is no normative content – on the contrary, it points to the need for doctrinal reconstruction.[15]

Achieving clarity of the term is undoubtedly hampered by the multitude of contexts in which it is used. In the CRA itself, the preamble contains the phrases: "cyber resilience of products with digital elements" (108), "cyber resilience at global level" (123), "cyber resilience at EU level" (1), "cyber resilience of economic operators" (128), "cyber resilience

11 The axiological aspects of digital transformation are further specified in the joint "European Declaration on Digital Rights and Principles for the Digital Decade" proclaimed by the European Parliament, the Council, and the European Commission. European Declaration on Digital Rights and Principles for the Digital Decade 2023/C 23/01 (OJ C 23, 23 January 2023), 1–7; Grażyna Szpor, "Prawa jednostki i wspólnoty w Cyfrowej Dekadzie" [Rights of Individuals and Communities in the Digital Decade], in *W trosce o dobro wspólnoty i jednostki – zagadnienia administracyjnoprawne. Księga jubileuszowa dedykowana Profesor Zofii Duniewskiej* [For the Good of the Community and the Individual: Administrative and Legal Issues. Jubilee Book Dedicated to Professor Zofia Duniewska], eds. Barbara Jaworska-Dębska et al. (Warsaw: Wolters Kluwer, 2024), LEX/el.

12 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 L 151, 7 June 2019), 15–69.

13 Regulation (EU) 2025/38 of the European Parliament and of the Council of 19 December 2024 laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cyber threats and incidents and amending Regulation (EU) 2021/694 (Cyber Solidarity Act) (OJ L, 2025/38, 15 January 2025).

14 Pier Giorgio Chiara, "Understanding the Regulatory Approach of the Cyber Resilience Act: Protection of Fundamental Rights in Disguise?," *European Journal of Risk Regulation* 16, no. 2 (2025): 469–84, https://doi.org/10.1017/err.2025.9.

15 Fredrik Björck et al. "Cyber Resilience – Fundamentals for a Definition," in *New Contributions in Information Systems and Technologies*, vol. 1, eds. Alvaro Rocha et al. (Cham: Springer, 2015), 311–16, https://doi.org/10.1007/978-3-319-16486-1_31; Kjell Hausken, "Cyber Resilience in Firms, Organizations and Societies," *Internet of Things* 11 (2020): 100204, https://doi.org/10.1016/j.iot.2020.100204; Wojciech R. Wiewiórowski. "Europejskie roumienie cyberodporności" [European Understanding of Cyber Resilience], in *Internet. Cyberodporność. Cyber Resilience*, eds. Agnieszka Gryszczyńska, Grażyna Szpor, and Wojciech R. Wiewiórowski (Warsaw: C.H. Beck, 2025), 95–104.

of artificial intelligence systems" (51), and in Article 33(2) "cyber resilience regulatory sandboxes."[16]

This may lead to the formulation of many contextual definitions of cyber resilience, but the frequent co-application of several acts limits their usefulness. It is also possible – omitting the prefix "cyber" at the beginning – to refer to the legal definitions of the term resilience, which, however, are also contextual in nature. EU Regulation 2021/2041 states that "resilience" means the ability to cope with economic, social, and environmental shocks or persistent structural changes in a fair, sustainable, and inclusive manner.[17] In contrast, Directive (EU) 2022/2557 of the European Parliament and of the Council defines resilience as the ability to "prevent, protect against, respond to, resist, mitigate, and absorb an incident, and adapt and recover from an incident."[18] The literature emphasizes that achieving an acceptable level of resilience requires preventive measures to identify threats before they cause adverse effects,[19] which aligns with the nearly 100 uses of the terms "threat" and "cyber threat" in the NIS2 Directive.[20] In general terms, resilience is the ability of an entity to continue achieving its intended objectives despite cyber incidents,[21] which includes the ability to detect and counter threats, respond quickly to undesirable events, and maintain business continuity.[22]

Cyber resilience, as shown by the results of multidisciplinary research, is considered in the contexts of IT systems, critical infrastructure, business processes, organizations, societies, nation states, the EU, and the global community. If we cannot agree on a single, universal answer to the question of how to understand cyber resilience, then the appearance of this term in law and official documents should be accompanied by explanations of its meaning in a given context, to reduce doubts and ensure uniformity in the application of law and the performance of public tasks. Integrating the non-contradictory elements of the analysis, carried out using the legal-dogmatic method, it can be concluded that:

> Cyber resilience is the ability to cope with security challenges related to the digital transformation. As a legal concept, it refers to products with digital elements as well as social and economic processes, information and political-organisational systems. It includes detecting and

16 Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) (OJ L, 2024/2847, 20 November 2024).

17 Regulation (EU) 2021/241 of the European Parliament and of the Council of 12 February 2021 establishing the Recovery and Resilience Facility (OJ L 57, 18 February 2021), 17–75, Article 2(5).

18 Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC (OJ L 333/164, 27 December 2022).

19 Sławomir Dygnatowski, "Cyber Security as a Foundation for the Security of Critical Infrastructure in the Context of Modern Threats," *Journal of Konbin* 50, no. 4 (2020): 317, https://doi.org/10.2478/jok-2020-0089.

20 Szafrański, ed., *Cyberbezpieczeństwo*, 295–306.

21 A related term is cyberworthiness, which is a measure of a system's resilience to cyber incidents (cyber-attacks) and can be applied to software and hardware components. "Cyber Resilience," Wikipedia, https://en.wikipedia.org/wiki/Cyber_resilience.

22 Dominika Skoczylas, "Wzmocnienie zdolności Unii Europejskiej w zakresie cyberbezpieczeństwa – cybersolidarność w kontekście cyberzagrożeń" [Strengthening the European Union's Cybersecurity Capabilities: Cyber Solidarity in the Context of Cyber Threats], *Europejski Przegląd Sądowy*, no. 12 (2024): 39–44.

> reducing threats, responding to undesirable events and achieving objectives despite various disruptions: intentional and accidental, natural and man-made.[23]

Such a reconstruction allows us to see that cyber resilience is not limited to a single area of regulation, but can integrate across areas.

For the purposes of the CRA, 51 definitions contained in Article 3 are used, including 15 definitions referring to seven previous EU acts: Regulation 2019/881 (cybersecurity, cyber threat), Directive 2022/2555 (incident, near miss, CSIRT designated as coordinator), Regulation 2016/679 (personal data), Regulation 2019/1020 (Union harmonization legislation,[24] market surveillance authority, recall, withdrawal), Regulation (EU) No 1025/2012 (international standard, European standard, harmonized standard), Regulation (EC) No 765/2008 (conformity assessment body), and Recommendation 2003/361/EC (micro-enterprises, small enterprises, and medium-sized enterprises). Article 3 also contains definitions that refer in part to the CRA itself (point 29 – notified body to Article 43) and its annexes (point 20 – support period, point 27 – conformity assessment, point 31 – CE marking).

The extensive system of references confirms that the CRA does not create an autonomous regime but integrates existing elements into a new normative framework. From the perspective of legal theory, this means that cyber resilience functions as a systemic category, organizing the relationships between dispersed instruments of EU law.

In addition, 37 new definitions apply to the CRA, which can be divided into three groups: (1) definitions relating to products and their components, (2) subjective definitions, and (3) objective definitions related to placing on the market and risks in cyberspace.

The first group includes the term contained in the title of the act and the cascading terms that make up its definition, as well as those used in their explanation. Article 3(1) of the CRA states that "product with digital elements" means a software or hardware product and its remote data processing solutions (including software or hardware components that are being placed on the market separately). "Remote data processing" means the processing of data at a distance, for the purposes of which the software has been designed and developed by the manufacturer or under the manufacturer's responsibility, and the absence of which would prevent the product with digital elements from performing one of its functions (point 2). "Software" means a part of an electronic information system, which consists of computer code (point 4).[25] "Electronic information sys-

---

[23] Grażyna Szpor, "Introduction," in *Internet. Cyberodporność. Cyber Resilience*, eds. Agnieszka Gryszczyńska, Grażyna Szpor, and Wojciech R. Wiewiórowski (Warsaw: C.H. Beck, 2025), LXI and publications cited therein.

[24] CRA Article 3(32) contains an exception to the rule adopted for cross-references, "x means x as defined in...," and states: "Union harmonisation legislation" means the Union provisions listed in Annex I to Regulation (EU) 2019/1020 and any other Union provisions harmonizing the conditions for the marketing of products to which that Regulation applies.

[25] In addition to the definition of software in Article 3(48) of the CRA, "free and open-source software" is also defined.

tem" means a system, including electrical or electronic equipment, capable of processing, storing, or transmitting digital data (point 7). "Hardware" means a physical electronic information system or its parts capable of processing, storing or transmitting digital data (point 5). "Component" means software or equipment intended for integration into an electronic information system (point 6). Integration may take the form of a "logical connection" (point 8), a "physical connection" (point 9), or an "indirect connection" (point 10), whereby any device that is connected to a network and serves as an entry point to that network is referred to as an "end point" (point 11). The structure of this part of the glossary exemplifies careful adherence to the principles of legislative technique and a desire to ensure both internal and external terminological consistency.

The second group clarifies, in the context of the CRA, the meaning of terms relating to entities, such as: economic operator (12), manufacturer (13), authorized representative (15), importer (16), distributor (17), consumer (18), and notifying authority (26) – already widely used in law. With regard to this group of terms, despite their definition, conflicts may arise when several acts are applied simultaneously. An exception is the original term "open-source software steward,' which does not appear previously in EU law and is broadly defined as:

> [A] legal person other than the manufacturer, that has the purpose or objective of systematically providing support on a sustained basis for the development of specific products with digital elements, qualifying as free and open-source software and intended for commercial activities, and that ensures the viability of those products (point 14).[26]

The third group of defined terms covers substantive aspects: "placing on the market" (21), "making available on the market" (22), and distinguishes between "intended purpose" (23), "reasonably foreseeable use" (24),[27] and "reasonably foreseeable misuse" (25), which, by overcoming the previous vagueness of the scope, may facilitate the achievement of the objectives of the act. This group also includes the terms "cybersecurity risk" (37) and "significant cybersecurity risk" (38). On eur-lex.pl, "cybersecurity risk" is translated into Polish as "ryzyko w cyberprzestrzeni" (risk in cyberspace). From a Polish perspective, this raises doubts because cyberspace has a legal definition unrelated to incidents,[28] and, for example, a corrigendum was made in Commission Delegated Regulation (EU) 2024/1366,[29] changing the Polish text from "ryzyko w cyber-

[26] On the CRA's attempt to balance cybersecurity obligations with the development of open-source solutions, see: Mattis van 't Schip, "The Cyber Resilience Act and Open-Source Software: A Fine Balancing Act," *Journal of Intellectual Property, Information Technology and E-Commerce Law* 16, no. 1 (2025) 73–87.

[27] An application that is not necessarily the intended purpose specified by the manufacturer in the user manual, promotional or sales materials and statements, as well as in technical documentation, but which is most likely to result from reasonably foreseeable human behavior, technical operations or interactions (which may refer to so-called "dual-use items") – civil and military.

[28] Act on Martial Law and the Powers of the Commander-in-Chief of the Armed Forces and the Principles of his Subordination to the Constitutional Authorities of the Republic of Poland (i.e., Journal of Laws 2025, item 504).

[29] Commission Delegated Regulation (EU) 2024/1366 of 11 March 2024 supplementing Regulation (EU) 2019/943 of the European Parliament and of the Council by establishing a network code on sector-specific rules for cybersecurity aspects of cross-border electricity flows, C/2024/1383 (OJ L, 2024/1366, 24 May 2024); Rectificatif au règlement délégué (UE) 2024/1366 de la Commission du 11 mars 2024 complétant le règlement

przestrzeni" (risk in cyberspace) to "ryzyko cyberbezpieczeństwa" (cybersecurity risk). However, it is worth considering the definition of cyberspace and the risks associated with it in EU law.[30]

An analysis of the 51 definitions contained in Article 3 of the CRA shows that the legislator is building a coherent, logical conceptual structure and "operationalizing" security requirements, but does not exhaust the ontological scope of cyber resilience. However, the comparison also shows that the cyber resilience of products with digital elements is built on the current conceptual framework of digital transformation and, on the other hand, this framework is specified for the future in a broader sense than just those products.

4. Scope and Structure of the Cyber Resilience Act

The legal basis for digital transformation in the European Union, including cybersecurity, is typically shaped by the adoption of prospective acts (strategies, plans) first, followed by a gradual transition to directives, creating cross-border information links and regulations. Such phases can also be distinguished in relation to cyber resilience. In the current phase, in which several EU directives, regulations and decisions already refer to resilience in cyberspace, the CRA is sometimes referred to as an instrument that closes the system, ensuring that hardware and software are placed on the market with as few vulnerabilities as possible, that manufacturers provide security updates throughout the product lifecycle, and that information on safe use is understandable and easily accessible.[31]

From a legal perspective, this closing function is demonstrated not only by the cross-referenced definitions discussed above. It is also confirmed by the reference to other regulations in the extensive preamble, which contains 130 recitals,[32] as well as numerous specific exemptions in the general provisions relating to the scope of the CRA, which are important for harmonious cooperation and the avoidance of conflicts of competence in the application of the law.[33]

Regulations of the European Parliament and of the Council are binding in their entirety and directly applicable in all Member States, as provided for in Article 71(2) of the CRA. The fact that "an act is binding in its entirety" excludes, as emphasized in doctrinal

(UE) 2019/943 du Parlement européen et du Conseil en établissant un code de réseau sur des règles sectorielles concernant les aspects liés à la cybersécurité des flux transfrontaliers d'électricité (OJ L, 2024/90558, 16 September 2024).

30 See: Grzegorz Pilarski, "Tackling Cyberspace Threats: The International Approach," *Security and Defence Quarterly* 12, no. 3 (2016): 100–17, https://doi.org/10.35467/sdq/103238.

31 Krzysztof Silicki, "Cyberodporność wspierana przepisami prawa UE: akt o cyberodporności (CRA) i dyrektywa NIS 2" [Cyber Resilience Supported by EU Laws: Cyber Resilience Act and NIS2 Directive], in *Internet. Cyberodporność. Cyber Resilience*, 105–18.

32 See preamble, recitals 117 and 118, and recital 46 et seq.

33 Grażyna Szpor and Paweł Hajduk, "Współdziałanie w egzekwowaniu przepisów z zakresu cyberbezpieczeństwa" [Cooperation in the Enforcement of Cybersecurity Regulations], in *Cyberbezpieczeństwo. Współpraca versus konfrontacja informacyjna* [Cybersecurity: Cooperation versus Informational Confrontation] ed. Bolesław Szafrański (Warsaw: Wojskowa Akademia Techniczna, 2025), 297–307.

interpretation, its "selective or incomplete" application.[34] However, the EU legislator itself establishes in many regulations the possibility of limiting or excluding the application of certain provisions in EU or national law, or of the national legislator shaping certain issues differently.[35]

The CRA applies – as provided for in Article 2(1), meticulously using the terms defined in Article 2 – "to products with digital elements made available on the market, the intended purpose or reasonably foreseeable use of which includes a direct or indirect logical or physical data connection to a device or network." However, as many as seven subsequent paragraphs of this article (2–8) precisely define the limits of application, first excluding in paragraphs 2–4 such products with digital elements to which the three previous EU regulations (2017/745, 2017/746, 2019/2144), products certified in accordance with Regulation (EU) 2018/1139, and products covered by Directive 2014/90. The fifth point provides for the possibility of limiting or excluding the application of the CRA to products with digital elements covered by other EU legislation establishing requirements relating to all or certain types of risk, if this is consistent with the general regulatory framework and sectoral legislation provides the same or a higher level of protection than the CRA. In this regard, the Commission is empowered to adopt delegated acts in accordance with Article 61 to supplement the CRA by specifying whether such a restriction or exemption is necessary and to what extent. Further exemptions from the application of the CRA concern certain spare parts made available on the market (6), as well as products developed or modified exclusively for national security or defense purposes (7), and specifically designed for processing classified information (7). Finally, it is stipulated that the obligations laid down in the CRA "shall not entail the supply of information the disclosure would be contrary to the essential interests of national security, public security or defence" (8).

The analysis shows, on the one hand, a complex network of interconnections and, on the other, a diversity of methods and criteria for limiting the scope of the new EU act. Cyber resilience is included in the CRA as a set of common requirements relating to the market for products with digital elements, which are specified in other EU and national legislation and technical standards. This horizontal approach should, therefore, not interfere with the adaptation of the protection of individual product categories with digital elements to different threats and risk levels. Therefore, the CRA is not a comprehensive regulation for the cyber resilience of products with digital elements, but it is a leading act that brings together standards for such products, which are scattered across many acts.

5. Structure of the CRA and Dates of Entry into Force and Application

The structure of the CRA – comprising general provisions, obligations of economic operators, conformity assessment, notification of bodies, market surveillance, and transitional

[34] Tomasz Jaroszyński, *Rozporządzenie Unii Europejskiej jako składnik systemu prawa obowiązującego w Polsce* [European Union Regulation as a Component of the Legal System in Force in Poland] (Warsaw 2011), LEX/el.

[35] Michał Czerniawski, "Art. 93," in *Akt o usługach cyfrowych. Komentarz*, eds. Dominik Lubasz and Monika Namysłowska (Warsaw: Wolters Kluwer, 2024), SIP LEX.

provisions[36] – corresponds to the classic model of a harmonization regulation. Transparency is enhanced by the transfer of specific issues to eight extensive annexes.

Digital economy operators implementing the numerous requirements established by the Cybersecurity Act and resulting from national implementations of the NIS 2 Directive should have stronger guarantees than before that the hardware and software on which their information infrastructure is built meet equivalent requirements throughout the EU. Various aspects of these changes have already been the subject of detailed consideration and assessment, including critical comments on the difficulties of rapidly implementing many new obligations.[37] In this context, it should be noted that the dates of publication, entry into force, and application should be permanent elements of the dogmatic analysis of a legal act. They can also be considered more broadly, in the context of legal culture, which is important for achieving the desired consistency, functionality, transparency, and certainty of the law.[38]

The CRA – as provided for in Article 71 – enters into force on the twentieth day following its publication in the Official Journal of the European Union (L 2024/2847), which took place on November 20, 2024, i.e., on December 10, 2024. This act shall take effect on December 11, 2027. However, Chapter IV (Articles 35–51) shall apply from June 11, 2026, and Article 14 shall apply from September 11, 2026.

The entry into force of an EU regulation on the twentieth day after its publication is now standard practice. In assessing the rationality of such a standard time lag between publication and entry into force, the acceleration and facilitation of access to information on the law, linked to the electronic format of official journals and the development of legal search systems, is of significant importance.

The time gap between the entry into force and the application of an act draws attention, on the one hand, to the traditional identity of these terms in national law[39] and, on the other hand, to the fact that in Union law, an adjustment period begins on the date of entry into force. As emphasized in the literature, this is to enable legislators in EU Member States to supplement the provisions of the Regulation with the necessary national provisions implementing EU legislation. For public authorities and other entities, however, this period is intended to allow them to adapt to the requirements of the new provisions. In fact, it is sometimes shorter for entities obliged to apply the Regulation's provisions, as many issues are clarified in national provisions adopted later.[40] The CRA has accepted that its application will generally commence three years after it enters into

---

36 I. The general provisions (Articles 1–12); II. Obligations of economic operators and provisions on free and open-source software (Articles 13–26); III. Conformity of products with digital elements (Articles 27–34); IV. Notification of conformity assessment bodies (Articles 35–51); V. Market surveillance and enforcement (Articles 52–60); VI. Delegated powers and committee procedure (Articles 61–62); VII. Confidentiality and penalties (Articles 63–65); VIII. Transitional and final provisions (Articles 66–71).

37 Szpor, Gryszczyńska, and Wiewiórowski, eds., *Internet. Cyberodporność. Cyber Resilience*.

38 Sławomira Wronkowska, "O stanowieniu i ogłaszaniu prawa oraz o kulturze prawnej" [On the Enactment and Promulgation of Law and on Legal Culture], *Państwo i Prawo*, no. 4 (2007): 3–15.

39 Sławomira Wronkowska and Maciej Zieliński, *Komentarz do zasad techniki prawodawczej* [Commentary on the Principles of Legislative Technique] (Warsaw: Wolters Kluwer, 2004), 110.

40 Paweł Fajgielski, "Artykuł 99," in *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*, 3rd ed., ed. Paweł Fajgielski (Warsaw: Wolters Kluwer, 2025), 794.

force. Therefore, the adjustment period seems long when compared, for example, to the General Data Protection Regulation, where it lasted two years. The assumption that it will be difficult and complicated is confirmed by the publications mentioned above.

The non-simultaneous commencement of the application of individual provisions of the new regulation is common in EU law. However, the need and possibility of early application of selected provisions may be questioned. It is, therefore, worth paying attention to the objectives, scope, and timetable for the early application of CRA provisions imposing obligations on public authorities and businesses.

A year and a half before the CRA comes into full effect, from June 11, 2026, Chapter IV, entitled "Notification of conformity assessment bodies," comprising as many as 17 articles (Articles 35–51), will apply. The rationale for this is already set out in Article 35, which stipulates that Member States shall notify the Commission and the other Member States of the bodies authorized to carry out conformity assessments in accordance with the CRA (paragraph 1) and shall endeavor to ensure that, by December 11, 2026 a sufficient number of notified bodies are designated in the Union to carry out conformity assessments, thereby avoiding bottlenecks and barriers to market entry (paragraph 2). To this end, each Member State shall designate a notifying authority (Article 36).

In addition, from September 11, 2026, the 10 comprehensive paragraphs of Article 14 CRA entitled "Reporting obligations of manufacturers" shall apply.[41] Paragraph 9 stipulates that, by December 11, 2025, the Commission shall adopt delegated acts in accordance with Article 61 of the CRA to supplement the CRA by specifying the conditions for applying cybersecurity considerations to the delay of the dissemination of notifications.[42] When preparing both draft delegated and implementing acts, the Commission is required to (as expressed in the operative part in paragraphs 9 and 10) cooperate with the CSIRT network established under Article 15 of Directive (EU) 2022/2555 and with ENISA, which will undoubtedly facilitate the clear establishment of a legal basis for this cooperation. During the adjustment period, the references in Chapter IV and Article 14 to provisions that will apply from December 2027 may raise doubts. However, it is worth noting that Article 61 of the CRA provides that the powers to adopt delegated acts, referred to, *inter alia*, in Article 14(9), shall be conferred on the Commission for a period of five years from December 10, 2024 (p. 2).[43] Before adopting a delegated act, the Commission shall consult experts designated by each Member State. A delegated act shall enter into force only if neither the European Parliament nor the Council has objected (p. 6).

The phased implementation of the provisions indicates that cyber resilience is understood as a process of building systemic capabilities, rather than a one-off state of compliance. The early start of the notification of conformity assessment bodies and

41 For a discussion of the CRA's model of vulnerability coordination and disclosure, see: Jukka Ruohonen and Paul Timmers, "Vulnerability Coordination under the Cyber Resilience Act," *Applied Cybersecurity & Internet Governance* 4, no. 1 (2025): 1–18, https://doi.org/10.48550/arXiv.2412.06261.

42 These are the notifications referred to in Article 16(2) of the CRA. Furthermore, as stated in paragraph 10, the Commission may, by means of implementing acts, specify the format and procedure for submitting the notifications referred to in Articles 14, 15, and 16.

43 The delegation of powers may be revoked at any time by the European Parliament or by the Council, by means of a decision, which shall not affect the validity of the delegated acts already in force.

the reporting obligations of manufacturers serves to create the institutional infrastructure necessary for the functioning of the market after 2027. The adjustment period is, therefore, a structural element of building systemic resilience, enabling the gradual internalization of new requirements by public authorities and businesses.

6. Conclusions

To meet the current challenges of digital transformation, in particular the development of the Internet of Things in the EU, horizontal cybersecurity requirements for products with digital elements have been established by a regulation of the European Parliament and of the Council.

The term "cyber resilience," contained in the short title of Regulation 2024/2847, has no legal definition, so its meaning needs to be established. It is used with rapidly increasing frequency in publications in various fields of science, but is explained in different ways. The relationship between cyber resilience and cybersecurity, and their place in the conceptual framework of digital transformation, remains unclear.

The legal and doctrinal analysis of the CRA, including its systemic interpretation, sets the framework for interpretation. The preamble confirms that the EU legislator refers to cyber resilience not only in relation to products with digital elements, but also in various other contexts. The manner in which the scope and exemptions in Article 2 are defined shows that the horizontal CRA is not a complete regulation for the cyber resilience of products with digital elements, but rather, a leading act that brings together the scattered standards relating to such products across many acts. The list of definitions shows that the cyber resilience of products subject to the regulation is built on a legally binding conceptual framework for digital transformation. On the other hand, this framework specifies the future in a broader scope than just products with digital elements. The extension of the time gap between entry into force and the start of full application highlights the new obligations of EU and national public authorities and businesses, the fulfillment of which is a necessary prerequisite for strengthening cyber resilience.

The CRA's analysis confirms the hypothesis that the concept of cyber resilience has untapped potential for increasing the consistency and transparency of the law, which is essential for its effectiveness. The result is a proposal to adopt a general definition of cyber resilience as a systemic category, a higher-order concept capable of integrating scattered sectoral regulations and performing an organizing function for digital transformation processes in legal doctrine. A starting point in this direction could be to adopt the definition that cyber resilience is the ability to cope with security challenges related to the digital transformation. As a legal concept, it refers to products with digital elements, as well as social and economic processes, information, and political-organizational systems. It includes detecting and reducing threats, responding to undesirable events and achieving objectives despite various disruptions: intentional and accidental, natural and man-made. Such a reconstruction also shows that cyber resilience is not limited to a single area of regulation, but has integrative potential.

An analysis of the abbreviated titles of EU regulations and directives, and their use in the practical interpretation and application of law in the area of digital transformation also leads to calls for a change in EU legislative principles, moving away from their adoption only in exceptional cases and, in addition, possibly indicating objectives and values in their content.

References

Björck, Fredrik, Martin Henkel, Janis Stirna, and Jelena Zdravkovic. "Cyber Resilience – Fundamentals for a Definition." In *New Contributions in Information Systems and Technologies*. Vol. 1, edited by Alvaro Rocha, Ana Maria Correia, Sandra Costanzo, and Luis Paulo Reis, 311–16. Cham: Springer, 2015. https://doi.org/10.1007/978-3-319-16486-1_31.

Chiara, Pier Giorgio. "Understanding the Regulatory Approach of the Cyber Resilience Act: Protection of Fundamental Rights in Disguise?." *European Journal of Risk Regulation* 16, no. 2 (2025): 469–84. https://doi.org/10.1017/err.2025.9.

Czerniawski, Michał. "Artykuł 93." In *Akt o usługach cyfrowych. Komentarz* [*Digital Services Act. Commentary*] edited by Dominik Lubasz and Monika Namysłowska. Warsaw: Wolters Kluwer, 2024. SIP LEX.

Dygnatowski, Sławomir. "Cyber Security as a Foundation for the Security of Critical Infrastructure in the Context of Modern Threats." *Journal of Konbin* 50, no. 4 (2020): 309–20. https://doi.org/10.2478/jok-2020-0089.

Fajgielski, Paweł. "Artykuł 99." In *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*, 3rd ed., edited by Paweł Fajgielski, 794. Warsaw: Wolters Kluwer, 2025.

Hausken, Kjell. "Cyber Resilience in Firms, Organizations and Societies." *Internet of Things* 11 (2020): 100204. https://doi.org/10.1016/j.iot.2020.100204.

Jaroszyński, Tomasz. *Rozporządzenie Unii Europejskiej jako składnik systemu prawa obowiązującego w Polsce* [European Union Regulation as a Component of the Legal System in Force in Poland]. Warsaw 2011. LEX/el.

Linkov, Igor, and Alexander Kott. "Fundamental Concepts of Cyber Resilience: Introduction and Overview." In *Cyber Resilience of Systems and Networks: Risk, Systems and Decisions*, edited by Alexander Kott and Igor Linkov, 1–25. Cham: Springer, 2019. https://doi.org/10.1007/978-3-319-77492-3_1.

Pilarski, Grzegorz. "Tackling Cyberspace Threats: The International Approach." *Security and Defence Quarterly* 12, no. 3 (2016): 100–17. https://doi.org/10.35467/sdq/103238.

Ruohonen, Jukka, and Paul Timmers. "Vulnerability Coordination under the Cyber Resilience Act." *Applied Cybersecurity & Internet Governance* 4, no. 1 (2025): 1–18. https://doi.org/10.48550/arXiv.2412.06261.

Silicki, Krzysztof. "Cyberodporność wspierana przepisami prawa UE: akt o cyberodporności (CRA) i dyrektywa NIS 2" [Cyber Resilience Supported by EU Laws: Cyber Resilience Act and NIS2 Directive]. In *Internet. Cyberodporność. Cyber Resilience*, edited by Agnieszka Gryszczyńska, Grażyna Szpor, and Wojciech R. Wiewiórowski, 105–18. Warsaw: C.H. Beck, 2025.

Skoczylas, Dominika. "Wzmocnienie zdolności Unii Europejskiej w zakresie cyberbezpieczeństwa – cybersolidarność w kontekście cyberzagrożeń" [Strengthening the European Union's Cybersecurity Capabilities: Cyber Solidarity in the Context of Cyber Threats]. *Europejski Przegląd Sądowy*, no. 12 (2024): 39–44.

Szafrański, Bolesław, ed. *Cyberbezpieczeństwo: redefinicja zagrożeń* [Cybersecurity: Redefining Threats]. Warsaw: Wojskowa Akademia Techniczna, 2023.

Szpor, Grażyna. "Introduction." In *Internet. Cyberodporność. Cyber Resilience*, edited by Agnieszka Gryszczyńska, Grażyna Szpor, and Wojciech R. Wiewiórowski, LXI. Warsaw: C.H. Beck, 2025.

Szpor, Grażyna. "Prawa jednostki i wspólnoty w Cyfrowej Dekadzie" [Rights of Individuals and Communities in the Digital Decade]. In *W trosce* o *dobro wspólnoty i jednostki – zagadnienia administracyjnoprawne*. *Księga jubileuszowa dedykowana Profesor Zofii Duniewskiej* [For the Good of the Community and the Individual – Administrative and Legal Issues. Jubilee Book Dedicated to Professor Zofia Duniewska], edited by Barbara Jaworska-Dębska, Monika Kapusta, Aneta Kaźmierska-Patrzyczna, Piotr Korzeniowski, Anna Król, Ewa Olejniczak-Szałowska, Agnieszka Rabiega-Przyłęcka, and Przemysław Wilczyński. Warsaw: Wolters Kluwer, 2024. LEX/el.

Szpor, Grażyna, and Paweł Hajduk. "Współdziałanie w egzekwowaniu przepisów z zakresu cyberbezpieczeństwa" [Cooperation in the Enforcement of Cybersecurity Regulations]. In *Cyberbezpieczeństwo. Współpraca versus konfrontacja informacyjna.* [Cybersecurity: Cooperation versus Informational Confrontation] ed. Bolesław Szafrański, 297–307. Warsaw: Wojskowa Akadema Techniczna, 2025.

van 't Schip, Mattis. "The Cyber Resilience Act and Open-Source Software: A Fine Balancing Act." *Journal of Intellectual Property, Information Technology and E-Commerce Law* 16, no. 1 (2025): 73–87.

Wiewiórowski, Wojciech R. "Europejskie rozumienie cyberodporności" [European Understanding of Cyber Resilience]. In *Internet. Cyberodporność. Cyber Resilience*, edited by Agnieszka Gryszczyńska, Grażyna Szpor, and Wojciech R. Wiewiórowski, 95–104. Warsaw: C.H. Beck, 2025.

Wikipedia. "Cyber Resilience." https://en.wikipedia.org/wiki/Cyber_resilience.

Wronkowska, Sławomira. "O stanowieniu i ogłaszaniu prawa oraz o kulturze prawnej" [On the Enactment and Promulgation of Law and on Legal Culture]. *Państwo i Prawo*, no. 4 (2007): 3–15.

Wronkowska, Sławomira, and Maciej Zieliński. *Komentarz do zasad techniki prawodawczej* [Commentary on the Principles of Legislative Technique]. Warsaw: Wolters Kluwer, 2004.