UDC: 351.817:004.738.5(4-672EU)
DOI: 10.5937/PDSC26013R

Valentina Ranaldi, PhD, Associate Professor
European Union Law, "Niccolò Cusano" University, Rome, Italy
email: valentina.ranaldi@unicusano.it
ORCID ID: 0000-0002-1542-4100

Simone Rinaldi, PhD, Adjunct Professor
University of Catania, Italy
email: simone.rinaldi@unict.it
ORCID ID: 0009-0005-6437-3310

THE REFORM OF THE EU CYBERSECURITY FRAMEWORK: BETWEEN MARKET INTEGRATION AND DIGITAL SECURITY[1]

Abstract: The ongoing reform of the European Union's Cybersecurity Act provides an opportunity to reconsider the legal foundations, regulatory evolution and strategic role of the European Union's cybersecurity framework. While the proposed amendments preserve the internal-market rationale underpinning Regulation (EU) 2019/881, they also reflect the growing importance of cybersecurity as an essential component of the Union's digital security architecture. Against this background, the article examines the relationship between Article 114 TFEU, the European cybersecurity certification framework and the broader evolution of Union cybersecurity regulation. It argues that the proposed reform does not establish a new autonomous Union competence but confirms the capacity of internal-market harmonisation to accommodate increasingly complex technological and strategic challenges. At the same time, it shows how European cybersecurity certification has progressively evolved from a market-integration instrument into a broader regulatory mechanism supporting digital security, trusted ICT supply chains and the Union's strategic objectives, while remaining within the limits of the competences conferred by the Treaties.

[1] Paragraphs 1, 2 and 3 of this paper were written by Valentina Ranaldi, while paragraphs 4 and 5 were written by Simone Rinaldi.

Keywords: *Article 114 TFEU; Cybersecurity Act; European cybersecurity certification; Internal market harmonisation; Strategic cybersecurity.*

1. INTRODUCTION

The progressive digitalisation of economic and social activities has profoundly reshaped the regulatory challenges facing the European Union. Digital technologies increasingly operate across integrated markets, evolve more rapidly than traditional legislative processes can respond, and generate effects extending well beyond national borders. As a consequence, the Union is increasingly required to develop legal frameworks capable of responding to rapidly evolving technological phenomena while preserving the proper functioning of the internal market and ensuring a high level of protection of the various public interests recognised under Union law. Rather than constituting an autonomous field of Union competence, the regulation of digital technologies has progressively become one of the principal instruments through which the Union pursues the objectives entrusted to it by the Member States under the Treaties, most notably the establishment and functioning of the internal market[2].

This evolution should not, however, be understood as reflecting the emergence of a general Union competence to regulate technological development. The growing economic and strategic importance of digital technologies does not, in itself, justify legislative intervention at Union level. In accordance with the principle of conferral enshrined in Article 5 TEU, the Union may act only within the limits of the competences conferred upon it by the Member States, and every legislative measure must therefore be linked to a specific legal basis capable of supporting the objectives

[2] See, first, Arts. 3(3) TEU, 26 and 114 TFEU. The progressive regulation of digital technologies through internal-market harmonisation reflects the broader evolution of Union action in response to digital transformation. See European Commission, Shaping Europe's Digital Future, COM(2020) 67 final, Brussels, 19 February 2020; European Commission, A European Strategy for Data, COM(2020) 66 final, Brussels, 19 February 2020; European Commission, 2030 Digital Compass: The European Way for the Digital Decade, COM(2021) 118 final, Brussels, 9 March 2021; Decision (EU) 2022/2481 of the European Parliament and of the Council of 14 December 2022 establishing the Digital Decade Policy Programme 2030, in OJ L 323, 19.12.2022. On the increasing reliance upon Art. 114 TFEU as the principal legal basis for regulating the Digital Single Market, see Engel (2025, pp. 13–28).

pursued by the Union legislature. The central legal question is therefore not whether the Union may regulate emerging technologies, but how the competences conferred by the Member States through the Treaties may be exercised so as to accommodate technological innovation while remaining consistent with the legal framework established by the Treaties[3].

Few areas of European digital regulation illustrate this broader evolution more clearly than cybersecurity. As digital infrastructures have become increasingly interconnected and economic activities progressively rely upon networked technologies, cybersecurity has evolved from a predominantly technical concern into a fundamental precondition for the functioning of the internal market. The security of digital products, services and infrastructures directly affects cross-border trade, consumer confidence, the provision of essential services and, more broadly, the competitiveness of the European digital economy. At the same time, the inherently transnational character of cyber threats demonstrates the limited effectiveness of fragmented national regulatory responses and reinforces the rationale for common Union action aimed at ensuring coherent regulatory conditions for the development and circulation of digital technologies throughout the internal market[4].

The evolution of European cybersecurity legislation provides a particularly appropriate case study through which to examine these broader

[3] The principle of conferral, enshrined in Art. 5(1) and (2) TEU, requires every exercise of Union legislative power to be based upon a competence expressly conferred by the Member States through the Treaties. As consistently held by the Court of Justice, the choice of the legal basis of a Union act must rest on objective factors amenable to judicial review, including its aim and content. See Court of Justice, 5 October 2000, Case C-376/98, *Germany v Parliament and Council*, ECLI:EU:C:2000:544, paras. 83–85; Court of Justice, 10 December 2002, Case C-491/01, *British American Tobacco*, ECLI:EU:C:2002:741, paras. 93–95; Court of Justice, 8 June 2010, Case C-58/08, *Vodafone and Others*, ECLI:EU:C:2010:321, paras. 32–34.

[4] On the close relationship between cybersecurity and the functioning of the Digital Single Market, as well as on the limits of fragmented national approaches, see González Fuster and Jasmontaite (2020, pp. 101, 107–108). The authors observe that ineffective cybersecurity policies may obstruct the functioning of the Digital Single Market and explain how the Union legislature established a link between cybersecurity and the internal market in order to address divergent national practices. See also Stewart Ferguson (2022, pp. 52–53), who analyses the Cybersecurity Act as a measure directed at improving the functioning of the internal market by increasing the level of cybersecurity and strengthening the capacity of organisations to resist and recover from cyber threats. This rationale is expressly reflected in 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), in OJ L 151, 7.6.2019, 15–69, especially Recitals 1–9 and 69–70 and Arts. 46(1) and 57(4).

legal dynamics. With the adoption of 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 (Cybersecurity Act), the Union established a permanent mandate for the ENISA and introduced an EU-wide cybersecurity certification framework for Information and Communication Technology (ICT) products, ICT services and ICT processes. Rather than laying down generally applicable substantive cybersecurity obligations for economic operators, the Regulation created a common framework for the development and recognition of European cybersecurity certification schemes, intended to strengthen trust in digital technologies, facilitate the free movement of certified products and services and reduce regulatory fragmentation across the internal market[5].

The rapid evolution of the technological, economic and geopolitical environment has, however, revealed a number of limitations of the existing framework. The increasing sophistication of cyber threats, the growing dependence of both public authorities and private operators upon digital infrastructures, the emergence of increasingly interconnected digital ecosystems and the strategic importance attributed to secure ICT supply chains have progressively expanded the role assigned to cybersecurity within the Union's internal-market policy.

Against this background, the Commission's Proposal for a Regulation repealing and replacing Regulation (EU) 2019/881 (COM(2026) 11 final) should not be regarded merely as a technical revision of the existing legislation. Rather, it reflects the continuing evolution of the Union's harmonisation strategy in response to profound technological change, while continuing to rely upon Article 114 TFEU[6].

[5] Regulation (EU) 2019/881, cit., Arts. 1(1), 46(1) and 49–54 and Recitals 67–78. See also Stewart Ferguson (2022, pp. 51–53).

[6] European Commission, *Proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Cybersecurity (ENISA), the European cybersecurity certification framework, and ICT supply chain security and repealing Regulation (EU) 2019/881 (The Cybersecurity Act 2)*, COM(2026) 11 final, Strasbourg, 20 January 2026, Explanatory Memorandum, Sections 1 and 2. The Commission identifies four principal problems addressed by the proposed revision: the misalignment between the Union's cybersecurity framework and stakeholders' needs in an increasingly hostile threat landscape; the stalled implementation of the European cybersecurity certification framework; the complexity and diversity of cybersecurity-related policies; and the increasing risks affecting ICT supply chains. It further expressly states that, in view of the evolving nature of cybersecurity threats and the increasing interdependence of Member

Scholarship has extensively examined, albeit largely in separate strands, the interpretation of Article 114 TFEU, the development of the Digital Single Market, the European cybersecurity certification framework and, more generally, the progressive expansion of Union cybersecurity regulation. These contributions have significantly enhanced the understanding of each of these dimensions. Nevertheless, the relationship among them has received comparatively limited attention, particularly as regards what the proposed reform of the Cybersecurity Act may reveal about the capacity of Article 114 TFEU to accommodate increasingly complex forms of digital regulation while remaining consistent with the system of competences conferred upon the Union by the Member States through the Treaties[7].

Against this background, the present article seeks to contribute to this discussion. It advances the argument that the proposed reform of the Cybersecurity Act should not be understood solely as an adaptation of European cybersecurity legislation to evolving technological challenges. Rather, it may also be regarded as a significant illustration of the flexibility of Article 114 TFEU as the legal basis for internal-market harmonisation, demonstrating how existing Treaty competences may support increasingly sophisticated forms of digital regulation without requiring any modification of the allocation of competences established by the Treaties. From this perspective, the evolution of European cybersecurity certification provides a particularly useful lens through which to analyse the relationship between technological innovation, market integration and the exercise of Union competences in the digital era.

The article therefore addresses two principal research questions. First, how does Article 114 TFEU continue to provide an appropriate legal basis for the progressive development of European cybersecurity regulation notwithstanding the profound technological transformations that have occurred since the adoption of the original Cybersecurity Act? Secondly,

States' digital systems, Art. 114 TFEU remains the justified legal basis for the proposed revision.

[7] On the increasingly extensive use of Art. 114 TFEU as the legal basis for Union measures governing the Digital Single Market, see Engel (2025, pp. 13–16, 27–28). On the European cybersecurity certification framework and its relationship with the functioning of the internal market, see Stewart Ferguson (2022, pp. 51–53). These contributions exemplify two distinct strands of scholarship concerning, respectively, the role of Art. 114 TFEU in Union digital regulation and the operation of the European cybersecurity certification framework; both predate the Commission's 2026 proposal and therefore do not examine the significance of that proposal for the adaptability of internal-market harmonisation to the evolving technological and strategic environment.

how does the ongoing reform of the European cybersecurity framework illustrate the evolving relationship between internal-market harmonisation, cybersecurity certification and the Union's broader strategic objectives, while remaining consistent with the limits of the competences conferred by the Treaties?

To answer these questions, the article adopts a doctrinal legal methodology based upon the analysis of the Treaties, the relevant secondary legislation, the case law of the Court of Justice of the European Union, the Commission's Proposal COM(2026) 11 final and the existing academic literature. Following this Introduction, Section 2 examines the evolution of Article 114 TFEU as the principal legal basis for European digital regulation. Section 3 analyses the European cybersecurity certification framework and the proposed reform in the broader context of the Union's internal-market harmonisation strategy. Section 4 broadens the analysis to the substantive-security and strategic dimensions of the evolving European cybersecurity framework. Finally, Section 5 draws together the principal findings and evaluates their implications for the future development of European cybersecurity law and for the interpretation of Union competences within the legal framework established by the Treaties.

2. Cybersecurity and the Internal Market: The Legal Framework of Union Action

The digital transformation of the European economy has progressively reshaped the conditions necessary for the proper functioning of the internal market. As cross-border economic activities, public services and critical infrastructures have become increasingly interconnected through digital technologies, ensuring a high level of cybersecurity has emerged as an essential condition for the effective functioning of the internal market[8]. This

[8] On the progressive development of the Union cybersecurity *acquis*, see, *inter alia*, Regulation (EU) 2019/881, cit.; 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), in OJ L 333, 27.12.2022; Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011, in OJ L 333, 27.12.2022; 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)

evolution has led to the gradual development of a comprehensive Union regulatory framework addressing different dimensions of cybersecurity. Yet the growing importance of cybersecurity does not, in itself, explain the legal framework within which the European Union has exercised its regulatory powers in this field. Since the Treaties do not confer upon the Union a general competence in matters of cybersecurity, understanding both the Cybersecurity Act and the proposal for its reform requires, as a preliminary step, identifying the legal basis and regulatory rationale underpinning Union action[9].

Indeed, the growing relevance of cybersecurity within Union law cannot be understood solely in light of the increasing sophistication of cyber threats. Rather, it reflects the profound transformation of the internal market driven by digitalisation. The free movement of goods, services, capital and data increasingly depends upon digital infrastructures that operate across national borders, making the security and reliability of networked systems a precondition for the effective exercise of the internal market freedoms. In such an environment, divergent national cybersecurity requirements are liable to create regulatory fragmentation, increase compliance costs for economic operators and undermine mutual trust in the security of digital products and services. It is precisely this cross-border dimension that explains why cybersecurity has progressively become an area in which Union action may legitimately pursue market integration through regulatory harmonisation, while simultaneously contributing to a high level of cybersecurity across the Union[10].

2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act), in OJ L, 2024/2847, 20.11.2024.

[9] See Art. 5(1) and (2) TEU. In the absence of a general competence in matters of cybersecurity, each legislative measure adopted in this field must be based upon a specific competence conferred upon the Union by the Member States through the Treaties. The increasing technological, economic or strategic importance of cybersecurity cannot, in itself, extend the scope of the competences attributed to the Union.

[10] The close relationship between cybersecurity and the proper functioning of the internal market is expressly reflected in Regulation (EU) 2019/881, cit., in particular Recitals 1–9, 69–70 and Arts. 1(1), 46 and 57, which link the establishment of a European cybersecurity certification framework to the reduction of market fragmentation and the improvement of the functioning of the internal market. The same rationale underpins the proposed reform. See European Commission, COM(2026) 11 final, cit., Explanatory Memorandum, Sections 1–2. The Commission explains that the proposal seeks to reduce regulatory fragmentation, improve the consistency and effectiveness of the European cybersecurity certification framework, strengthen the resilience of the Union's digital ecosystem and enhance the security of ICT supply chains while continuing to rely upon Art. 114 TFEU as its legal basis.

The progressive emergence of cybersecurity as a regulatory priority does not alter the legal framework governing the allocation and exercise of Union competences. In accordance with the principle of conferral, the European Union may legislate only where the Treaties have conferred the necessary competence and within the limits established therein[11]. Since the Treaties contain no specific legal basis empowering the Union to adopt a comprehensive cybersecurity policy, legislative action in this field has necessarily been anchored in existing Treaty competences. Against this background, Article 114 TFEU has assumed particular significance. Rather than establishing a general competence in matters of cybersecurity, it provides the legal basis for the approximation of national laws where divergences between Member States are liable to hinder the establishment or functioning of the internal market or give rise to appreciable distortions of competition. Consequently, the legal justification for Union measures in the field of cybersecurity lies not in the objective of enhancing cybersecurity considered in isolation, but in the need to remove or prevent obstacles to the functioning of the internal market through legislative harmonisation[12].

The Court of Justice has repeatedly interpreted Article 114 TFEU as conferring broad legislative powers upon the Union legislature, while at the same time defining clear conditions governing its use. The mere existence of disparities between national legal systems is not, in itself, sufficient to justify recourse to Article 114 TFEU. Rather, it must be demonstrated that actual or potential divergences between national rules are liable to create obstacles to the exercise of the fundamental freedoms or to give rise to

[11] See Art. 5(1) and (2) TEU. The principle of conferral requires the Union to act only within the limits of the competences conferred upon it by the Member States through the Treaties. Competences not conferred upon the Union remain with the Member States.

[12] Art. 114(1) TFEU empowers the Union legislature to adopt measures for the approximation of national provisions which have as their object the establishment and functioning of the internal market. Recourse to that provision requires the measure genuinely to pursue that objective and to contribute to removing obstacles to the exercise of the fundamental freedoms or appreciable distortions of competition. Article 114 TFEU may also support measures designed to prevent future obstacles resulting from divergent national legislation, provided that the emergence of such obstacles is likely and that the measure is intended to prevent them. Where those conditions are satisfied, the fact that the measure simultaneously pursues a high level of protection of another interest recognised under Union law does not preclude reliance upon Art. 114 TFEU. See Court of Justice, *Germany v Parliament and Council*, C-376/98, cit., paras. 83–88; Court of Justice, *British American Tobacco*, C-491/01, cit., paras. 60–62; Court of Justice, *Vodafone and Others*, C-58/08, cit., paras. 32–33 and 36–37.

appreciable distortions of competition within the internal market[13]. At the same time, the Court has consistently recognised that measures adopted on the basis of Article 114 TFEU may legitimately pursue additional public interest objectives, including the protection of public health, consumers or the environment, provided that the approximation of national laws genuinely contributes to improving the conditions for the establishment and functioning of the internal market[14]. This functional interpretation of Article 114 TFEU has progressively enabled the Union legislature to regulate increasingly complex sectors characterised by significant cross-border externalities, of which cybersecurity constitutes a particularly significant contemporary example.

Against this legal background, the Cybersecurity Act should not be regarded as establishing an autonomous Union policy in the field of cybersecurity. Rather, it exemplifies the broader regulatory approach through which the Union legislature addresses emerging technological challenges by relying upon the legal techniques of internal-market harmonisation. The objective pursued by the Regulation is undoubtedly to enhance cybersecurity throughout the Union; however, its legal basis lies in its contribution to the establishment and functioning of the internal market pursuant to Art. 114 TFEU. This distinction is not merely formal. It determines both the scope of the Union's regulatory powers and the limits within which the Union legislature may further develop the European cybersecurity framework. From this perspective, the proposed reform of the Cybersecurity Act does not represent a change in the legal basis of Union action, but rather a further stage in the evolution of a harmonised regulatory

[13] See Court of Justice, *Germany v Parliament and Council*, C-376/98, cit., paras. 84–86; Court of Justice, *British American Tobacco*, C-491/01, cit., paras. 60–62; Court of Justice, *Vodafone and Others*, C-58/08, cit., paras. 32–37. As the Court has consistently held, Art. 114 TFEU may be relied upon where divergences between national rules are liable to obstruct the exercise of the fundamental freedoms or to give rise to appreciable distortions of competition, including where the emergence of such obstacles is likely and the measure is intended to prevent them.

[14] The Court has consistently recognised that measures adopted on the basis of Art. 114 TFEU may simultaneously pursue a high level of protection of other interests recognised by the Treaties, provided that they genuinely contribute to improving the conditions for the establishment and functioning of the internal market. See Court of Justice, *British American Tobacco*, C-491/01, cit., para. 62; Court of Justice, *Philip Morris Brands and Others*, C-547/14, cit., paras. 58–61. See also Art. 114(3) TFEU, which requires the Commission, in its proposals concerning health, safety, environmental protection and consumer protection, to take as a base a high level of protection.

framework designed to reconcile market integration with an increasingly high level of cybersecurity[15].

3. The European Cybersecurity Certification Framework and the Reform of the Cybersecurity Act

Regulation (EU) 2019/881 constitutes the principal legislative expression of the harmonisation strategy examined in the previous section. Its principal innovation is the establishment of a European cybersecurity certification framework. Rather than imposing harmonised technical requirements directly upon manufacturers and service providers, the Cybersecurity Act established a legal framework for the development and recognition of European cybersecurity certification schemes. In doing so, the Regulation sought to address one of the principal sources of fragmentation within the digital internal market, namely the coexistence of multiple national certification systems characterised by differing procedures, assurance requirements and levels of recognition. By replacing this fragmented landscape with a coherent European certification architecture, the Union legislature sought simultaneously to facilitate the free movement of ICT products, ICT services and ICT processes and to strengthen confidence in their cybersecurity throughout the internal market[16].

Unlike traditional harmonisation measures, the European cybersecurity certification framework does not establish uniform substantive cybersecurity requirements directly applicable to ICT products, ICT services or ICT processes. Instead, it creates a common legal framework within which European cybersecurity certification schemes may be developed according to uniform procedural rules and recognised throughout the Union. The Regulation thereby distinguishes between the legal framework governing certification and the technical specifications incorporated into individual

[15] This understanding is consistent with both Regulation (EU) 2019/881, cit., in particular Recitals 1–9, 67–70 and Art. 1(1), and the Commission's Proposal COM(2026) 11 final, cit., Explanatory Memorandum, Sections 1–2. The Proposal presents the reform as a measure intended to improve the functioning of the internal market by strengthening the European cybersecurity certification framework, reducing regulatory fragmentation, enhancing trust in digital products and services, and reinforcing the resilience and security of ICT supply chains, while continuing to rely upon Art. 114 TFEU as its legal basis.

[16] Regulation (EU) 2019/881, cit., Recitals 4, 7–9 and 67–78 and Arts. 46–54. The Regulation establishes a European cybersecurity certification framework intended to reduce the fragmentation resulting from multiple national certification schemes by facilitating the mutual recognition of European cybersecurity certificates and strengthening trust in ICT products, ICT services and ICT processes throughout the internal market.

European cybersecurity certification schemes, allowing those specifications to evolve in response to technological developments while preserving the uniform legal effects attached to certification throughout the Union. This model reflects the increasing reliance of Union internal-market legislation upon regulatory mechanisms capable of combining legal certainty with technological flexibility, thereby reducing barriers to cross-border economic activity without incorporating detailed technical specifications directly into the legislative act[17].

The governance of the European cybersecurity certification framework reflects the Union's attempt to reconcile regulatory uniformity with the need for technical expertise and adaptability. The Commission is empowered to adopt European cybersecurity certification schemes through implementing acts within a structured institutional framework involving ENISA and the European Cybersecurity Certification Group (ECCG). ENISA performs a central technical function by preparing candidate certification schemes and providing scientific and technical expertise throughout the certification process, whereas the ECCG, composed of representatives of the national cybersecurity certification authorities, assists and advises the Commission while facilitating cooperation and the exchange of information among the competent national authorities. This institutional design combines centralised regulatory decision-making with decentralised technical expertise, seeking to ensure both the uniform application of European cybersecurity certification schemes throughout the internal market and their capacity to adapt to technological developments[18].

[17] Regulation (EU) 2019/881, cit., Arts. 46–54. Under the Regulation, European cybersecurity certification schemes specify, inter alia, the categories of ICT products, ICT services or ICT processes covered, the applicable cybersecurity requirements, the evaluation methods, the assurance levels and the conditions governing the issuance, maintenance, suspension and withdrawal of European cybersecurity certificates. By establishing a common procedural framework while leaving the technical specifications to the individual certification schemes, the Regulation enables those specifications to evolve in response to technological developments without requiring legislative amendment.

[18] Regulation (EU) 2019/881, cit., Arts. 47–53. The Commission is empowered to adopt European cybersecurity certification schemes by means of implementing acts. ENISA prepares candidate schemes and provides scientific and technical expertise throughout the certification process, while the European Cybersecurity Certification Group (ECCG), composed of representatives of the national cybersecurity certification authorities, assists and advises the Commission and facilitates cooperation and the exchange of information among the competent national authorities, thereby contributing to the consistent implementation and development of the European cybersecurity certification framework.

A further distinctive feature of the European cybersecurity certification framework is the introduction of three harmonised assurance levels—basic, substantial and high—designed to indicate the degree of confidence that an ICT product, ICT service or ICT process has been evaluated in accordance with the cybersecurity requirements established by the relevant European cybersecurity certification scheme. Rather than expressing different levels of product quality, these assurance levels correspond to progressively more demanding evaluation procedures and provide users, public authorities and economic operators with a common benchmark for assessing cybersecurity risks across the internal market. Their harmonised definition contributes to enhancing transparency, legal certainty and mutual trust while reducing the fragmentation previously resulting from divergent national certification methodologies. The assurance levels therefore constitute an essential component of the Union's objective of ensuring the mutual recognition and practical effectiveness of European cybersecurity certification[19].

The European cybersecurity certification framework may therefore be understood as a mechanism of regulatory harmonisation based upon mutual trust rather than upon the exhaustive harmonisation of technical requirements. The Cybersecurity Act neither centralises conformity assessment activities nor replaces the national authorities responsible for certification. Instead, it establishes common procedural rules, harmonised assurance levels and uniform legal effects capable of fostering confidence in certification outcomes throughout the Union. The effectiveness of the system therefore depends less upon the substantive uniformity of cybersecurity solutions than upon the credibility, transparency and consistency of the procedures through which conformity is assessed. From this perspective, European cybersecurity certification operates as a legal instrument designed to facilitate the free movement of ICT products, ICT services and ICT processes within the internal market by reducing information asymmetries and strengthening confidence among economic operators, public authorities and end users[20].

[19] Regulation (EU) 2019/881, cit., Art. 52. The Regulation establishes three assurance levels—basic, substantial and high—corresponding to increasing degrees of confidence that an ICT product, ICT service or ICT process complies with the cybersecurity requirements specified in the relevant European cybersecurity certification scheme. The assurance level reflects the depth and rigour of the evaluation process rather than the intrinsic quality of the certified product, service or process, thereby providing a harmonised methodology for assessing cybersecurity properties throughout the Union.

[20] Regulation (EU) 2019/881, cit., Recitals 4, 7–9 and 67–70 and Arts. 46–54. The European cybersecurity certification framework is intended to facilitate the free movement

The coherent legal architecture established by Regulation (EU) 2019/881 has not prevented significant challenges from emerging in the practical implementation of the European cybersecurity certification framework. The development of European cybersecurity certification schemes has progressed more slowly than originally anticipated, while the coexistence of sector-specific Union legislation, voluntary certification mechanisms and residual national requirements has continued to generate legal complexity for economic operators. At the same time, the rapid evolution of the digital economy—including the increasing relevance of cloud computing, connected devices, artificial intelligence and increasingly complex ICT supply chains—has exposed regulatory challenges that were only partially foreseeable when the Cybersecurity Act was adopted in 2019[21].

These developments have not called into question the underlying rationale of the European certification framework. Rather, they have highlighted the need to refine its institutional and regulatory mechanisms in order to preserve its effectiveness in a significantly transformed technological and strategic environment. It is against this background that the Commission's proposal to repeal and replace Regulation (EU) 2019/881 should be understood. Rather than departing from the original model, the proposed reform seeks to strengthen the functioning of the existing certification framework while preserving its legal basis and its internal-market rationale[22].

A first limitation concerns the pace at which European cybersecurity certification schemes have been developed and implemented. Although the Cybersecurity Act established a comprehensive legal framework for Union-wide certification, the practical deployment of European cybersecurity

of ICT products, ICT services and ICT processes by establishing common procedural rules, harmonised assurance levels and the mutual recognition of European cybersecurity certificates throughout the Union. In doing so, the Regulation seeks to strengthen transparency, comparability and confidence in certification outcomes while preserving the flexibility of the certification schemes to accommodate technological developments.

[21] European Commission, COM(2026) 11 final, cit., Explanatory Memorandum, Sections 1–2. For an early critical assessment of the original European cybersecurity certification framework, identifying both the absence, at that stage, of publicly available European cybersecurity certification schemes and significant shortcomings in the minimum-security objectives established by the Cybersecurity Act, see Stewart Ferguson (2022, pp. 52–53, 108–114).

[22] The Proposal continues to rely upon Art. 114 TFEU and expressly presents the reform as an evolution of the existing regulatory framework rather than the introduction of a new Union competence in the field of cybersecurity. See European Commission, COM(2026) 11 final, cit., Explanatory Memorandum, Sections 1–3.

certification schemes has progressed more slowly than originally envisaged, thereby limiting the framework's capacity to support the functioning of the digital internal market. Delays in the adoption of certification schemes have reduced the availability of harmonised certification mechanisms for emerging technologies and have consequently limited the ability of economic operators to rely upon a coherent certification framework across the Union[23]. Recognising these shortcomings, the Commission's 2026 proposal seeks to streamline the development and maintenance of European cybersecurity certification schemes by simplifying procedural arrangements, clarifying institutional responsibilities and strengthening ENISA's operational role. The objective is not to redefine the certification model established in 2019, but to improve its responsiveness to technological innovation and market needs while preserving the coherence of the Union certification framework[24].

A second and more significant development concerns the increasing attention devoted to the cybersecurity of ICT supply chains. The original architecture of Regulation (EU) 2019/881 was conceived primarily with a view to facilitating the certification of individual ICT products, ICT services and ICT processes. Subsequent technological and geopolitical developments, however, have demonstrated that cybersecurity risks frequently arise not from isolated components but from the complex interdependencies characterising ICT supply chains and interconnected digital infrastructures. The Commission's proposal acknowledges this evolution by strengthening the role of European cybersecurity certification within a broader regulatory framework aimed at enhancing the resilience and security of the Union's digital ecosystem. In doing so, it does not alter the fundamental nature of the certification framework. Instead, it adapts its operation to a technological environment in which the effective functioning of the internal market increasingly depends upon the security and reliability

[23] European Commission, COM(2026) 11 final, cit., Explanatory Memorandum, Sections 1–2. See also Commission Staff Working Document accompanying the Proposal, SWD(2026) 2 final, in particular the assessment of the European Cybersecurity Certification Framework (ECCF), which documents the delays in the operationalisation of certification schemes, the procedural complexity of the existing framework and the concerns expressed by stakeholders regarding governance and implementation.

[24] For an early critical assessment of the original certification framework, see Stewart Ferguson (2022, pp. 52–53, 108–114). See also Lotito and Dalli (2026, p. 9), who observe that the European Cybersecurity Certification Framework has advanced more slowly than initially foreseen and report stakeholders' concerns regarding delays in the development of certification schemes, process transparency and long-term planning.

of interconnected ICT supply chains rather than upon the characteristics of individual ICT products alone[25].

The amendments proposed in 2026 do not alter the legal rationale underlying the European cybersecurity certification framework. On the contrary, they confirm the central role of certification as a regulatory technique through which the Union seeks to strengthen the functioning of the internal market without resorting to the exhaustive harmonisation of technical cybersecurity requirements. Rather than prescribing uniform technological solutions, the certification framework establishes common legal conditions governing the assessment, certification and recognition of ICT products, ICT services and ICT processes throughout the Union. Its primary function is therefore not to replace technological innovation with regulatory uniformity, but to ensure that certification outcomes are produced according to transparent, consistent and comparable procedures capable of fostering mutual trust and facilitating the functioning of the internal market[26].

From this perspective, the European cybersecurity certification framework illustrates a broader evolution in Union internal-market legislation. As technological innovation continues to accelerate and become more complex, legislative harmonisation is no longer pursued exclusively through the detailed approximation of technical rules[27]. Instead, the Union

[25] European Commission, COM(2026) 11 final, cit., Explanatory Memorandum, Sections 1–3. The Proposal explains that the significant evolution of the cybersecurity threat landscape, the growing strategic importance of ICT supply chains and the increasing interdependence of digital infrastructures require a strengthening of the European cybersecurity certification framework while preserving its internal-market legal basis.

[26] Regulation (EU) 2019/881, cit., Recitals 4, 7–9 and 67–70 and Arts. 46–54. The European cybersecurity certification framework establishes common procedural rules, harmonised assurance levels and Union-wide legal effects for European cybersecurity certificates, while leaving the applicable technical requirements and evaluation methods to the individual European cybersecurity certification schemes. On the use of certification and conformity-assessment mechanisms within the broader architecture of Union cybersecurity legislation, see Chiara (2022a, pp. 262–263). Chiara analyses how Union product legislation increasingly combines generally applicable legal requirements with harmonised technical standards and European cybersecurity certification schemes capable of supporting presumptions of conformity. See also Brighi and Chiara (2021, pp. 21, 18–42), which analyses the progressive recognition of cybersecurity as a collective interest within the evolving legal framework of the European Union.

[27] On the broader development of risk-based approaches in Union digital regulation, see De Gregorio and Dunn (2022, pp. 473–500). The authors examine the emergence and different forms of risk-based regulation across Union digital legislation, highlighting its role as a

legislature establishes common legal frameworks governing the procedures through which compliance is assessed, certified and recognised throughout the internal market, while allowing the relevant technical specifications to evolve within that framework. European cybersecurity certification exemplifies this regulatory technique. It provides a common legal structure within which technical requirements may be progressively adapted while preserving the legal certainty, transparency and mutual trust necessary for the effective functioning of the digital internal market. The proposed reform confirms, rather than transforms, this model by adapting its institutional and procedural mechanisms to an increasingly interconnected technological environment. Accordingly, it should not be understood as marking a departure from the legal model established by Regulation (EU) 2019/881. Rather, it confirms the continuing reliance of the Union legislature upon internal-market harmonisation as the legal framework within which cybersecurity objectives are pursued. What has evolved is not the legal basis of Union action, but the technological, economic and strategic environment in which that action operates[28].

4. The Strategic and Technical Evolution of the European Cybersecurity Framework

Building upon the legal framework examined in the previous sections, the following analysis focuses on the broader strategic and operational implications of the evolving European cybersecurity framework. Particular attention is devoted to the role of cybersecurity certification within the Union's wider digital security architecture and to the interaction between the

regulatory technique for addressing the challenges posed by rapidly evolving digital technologies.

[28] European Commission, COM(2026) 11 final, cit., Explanatory Memorandum, Sections 1–3. The proposed reform preserves the certification framework as a system based upon European schemes, common procedural requirements, assurance levels, conformity assessment and Union-wide recognition, while modifying its institutional and operational mechanisms in response to technological and market developments. On the broader regulatory technique whereby Union legislation lays down essential or common legal requirements while technical specifications are developed and adapted through standardisation and conformity-assessment processes, see Vallejo (2021, pp. 196–197, 205–206). Vallejo reconstructs the transition from detailed legislative technical specifications to common legal requirements supplemented by adaptable standards and examines the emergence of more flexible and responsive regulatory techniques within internal-market law.

Cybersecurity Act and the more recent legislative initiatives adopted in response to the evolving cyber threat landscape.

Certification as a Substantive Security Guarantee, Not Merely a Harmonisation Technique

The most misleading reading reduces the European Cybersecurity Certification Schemes to a mechanism of mutual recognition among Member States, functional only to the circulation of ICT products and services. This obscures their primary, substantively securitarian function[29]. Under Articles 46-47 and 51 of Regulation (EU) 2019/881, certification schemes set technical requirements across increasing assurance levels – basic, substantial and high – corresponding to progressively more significant risk. This translates the "security by design" approach into a verifiable legal obligation and overcome the divide between security as engineering practice and security as regulatory compliance (Bygrave, 2021, p. 126), in a convergence between product-safety law and cybersecurity law. Recent literature regards this overcoming and this innovation as distinctive of EU digital regulation (Chiara, 2022b, pp. 130–131). The EUCC (European Common Criteria-based Cybersecurity Certification Scheme), operational since 2025 under Commission Implementing Regulation (EU) 2024/482, confirms this interpretation, applying the Common Criteria methodology (ISO/IEC 15408) to hardware, software and components including microprocessors and smart cards, in a technical-legal risk-management grid now placed by Italian legal doctrine among the "security by design" instruments of information technology law (Finocchiaro, 2023).

The 2025-2026 Reforms: From Managed Security Services to the January 2026 Comprehensive Revision

Since 2025 this framework has undergone a twofold reform. Regulation (EU) 2025/37 of 19 December 2024 enabled certification schemes for "managed security services" – incident response, penetration testing, security audits and consultancy – shifting certification's centre of gravity from products to providers of cyber services, with a corresponding

[29] On the broader conceptual dimension of cybersecurity as a matter of public interest, see Taddeo (2019, pp. 349–354). Taddeo cautions against treating cybersecurity as an undifferentiated public good and argues, more specifically, that the robustness of digital systems should be treated as a public good in view of its essential role for information societies and the public interest.

expansion of ENISA's mandate; Commission Implementing Regulation (EU) 2024/3143 simultaneously reorganised notification of conformity assessment bodies through the NANDO system. More significant is the comprehensive revision proposal presented by the Commission in January 2026, following the Regulation's five-yearly evaluation (European Parliamentary Research Service [EPRS], 2026). Beyond addressing the slow, fragmented adoption of individual schemes, it introduces a horizontal, Union-level ICT supply-chain security regime, providing for the designation of high-risk suppliers, identification of critical ICT assets, and harmonised prohibitions and mitigation measures for electronic communications networks (Bird & Bird, 2026; Covington & Burling, 2026), together with binding development timelines, four-yearly scheme review, and Commission power to withdraw obsolete schemes (Digital Watch Observatory, 2026; Palmieri, 2026).

The Strategic and Geopolitical Dimension: Regulatory Mercantilism, Hybrid Warfare and Supply-Chain Sovereignty

This reform trajectory cannot be understood without situating it within the broader geopoliticisation of EU technology policy. Recent literature describes the Union's perceived dependence on externally produced technologies as a structural vulnerability that increasingly merges economic and security rationales into "regulatory mercantilism": critical technological capacity is either relocated within EU territory or brought under the Union's regulatory reach (Farrand, Carrapico, & Turobov, 2024). Certification illustrates this starkly: the microprocessors and other hardware covered by the EUCC scheme are overwhelmingly manufactured outside the Union, so that the Cybersecurity Act's assurance levels function simultaneously as technical safeguards and as instruments of control over supply chains the Union cannot physically relocate (Farrand et al., 2024). This would open a much wider discussion on the strategic autonomy of the EU, which appears, today, far to be reached.

This logic acquires a military inflection once cyber operations are read, as EU institutions increasingly read them, as one line of effort within a broader hybrid-warfare toolbox. Russia's cyber operations against Ukraine, described by the Commission as a strategy that preceded and accompanied the land invasion, are treated as a paradigm shift in assessing the Union's collective cyber-crisis management capacity. This logic is running through the Cyber Solidarity Act and, arguably, through the high-risk-supplier regime now proposed (Farrand et al., 2024). Beyond Ukraine, sabotage of

undersea data and energy cables in the Baltic Sea and probing of critical infrastructure attributed to state-linked actors are read as evidence that hybrid aggression no longer respects the boundary between the cyber and the physical domain (European Council on Foreign Relations, 2025). Indeed, the border between cyber and kinetic military operations is evanishing. The designation of high-risk suppliers in the January 2026 proposal – indebted to the precedent of the EU's 5G Cybersecurity Toolbox – accordingly turns certification into an instrument of what recent commentary now describes as EU technological sovereignty (Farrand et al., 2024).

The resulting paradox is that this securitisation of certification and supply-chain policy still travels through the same legal vehicle – Article 114 TFEU internal-market harmonisation – designed for the considerably more modest objective of removing barriers to intra-European trade. Whether a single-market instrument can bear the weight of a genuinely strategic function, without diluting its security ambitions to market-making constraints or stretching Article 114 TFEU beyond its constitutional purpose, is likely to remain among the more contested questions following the reform's adoption.

The Cyber Solidarity Act: Collective-Response Logic and the Limits of Internal-Market Competence

This strategic shift is clearest in Regulation (EU) 2025/38, the Cyber Solidarity Act. It was adopted together with the managed-security-services reform of the Cybersecurity Act and has been in force since February 2025. Unlike the Cybersecurity Act and the Cyber Resilience Act, this Regulation does not rely on Article 114 TFEU. Instead, it rests on two other legal bases: Article 173(3) TFEU, on EU industrial policy, and Article 322(1)(a) TFEU, on budgetary measures. The reason is straightforward: its main tools – a Cybersecurity Alert System, a Cybersecurity Emergency Mechanism, and a Cybersecurity Reserve of pre-committed incident response providers – could not convincingly be presented as market harmonisation (Villani, 2025). This is not a minor technical detail. It shows that internal-market competence, however flexible, has reached its limit in a field that has traditionally belonged to national security. Indeed, Article 114 TFEU has itself been criticised as an increasingly strained tool for measures whose real purpose is security rather than trade (Varju, 2020).

The link between this Regulation and the collective-defence dimension of EU law is explicit. Its emergency mechanism is meant to work alongside

two other provisions: the mutual defence clause of Article 42(7) TEU, which applies when a Member State suffers armed aggression, and the solidarity clause of Article 222 TFEU, which covers terrorist attacks and man-made disasters (Villani, 2025). One question remains genuinely open in international law: can a large-scale cyber operation count as an "armed attack" under Article 42(7) TEU? The answer depends on the scale and effects of the operation, not on the means used to carry it out (Delerue, 2020; Kilovaty, 2022, p. 251). If the event is considered an armed attack or not is strictly connected to other factor, such as the political implication, the kinetic effect on people and infrastructure, and, as mentioned before, on the blurry line of ambiguity which is pivotal in hybrid warfare. The 2020 SolarWinds incident is often cited as the clearest test of this threshold. In that case, a backdoor hidden in widely used network-management software gave state-linked actors access to many public and private organizations across the transatlantic space. It offers a preview of the kind of large-scale, supply-chain-based incident that the Cyber Solidarity Act's Reserve is designed to address (Coco, Dias, & van Benthem, 2022; Villani, 2025).

Yet the Regulation also limits its own ambitions. A series of "non-affectation clauses" make Union intervention conditional on the willingness of the affected Member State, and Article 4(2) TEU still leaves each State with exclusive responsibility for its own national security (Villani, 2025). Together with the Cybersecurity Act reforms discussed above, the Cyber Solidarity Act completes a broader picture. The Union now combines market harmonisation, technical certification, supply-chain security, and an emerging capacity for collective cyber response, without ever fully reaching the language of collective defense found in Article 42(7) TEU. This overall trajectory has been described as part of a wider affirmation of "EU digital sovereignty". The Commission has used this notion since 2020, increasingly to justify giving the supranational level instruments that, from a strictly internal-market perspective, sit uneasily with the principle of conferral (Barrinha & Christou, 2022, p. 356; Villani, 2025).

Certification, Presumption of Conformity and Residual Fragmentation: The Cybersecurity Act, NIS2 and the Cyber Resilience Act

There is a further point to consider: how does the Act fit within the wider EU cybersecurity ecosystem? This ecosystem also includes Directive (EU) 2022/2555 (NIS2) and Regulation (EU) 2024/2847 (the Cyber Resilience Act). Recent commentary treats these three instruments as parts of a single regulatory design. Together, they combine a horizontal, risk-

based and product-safety approach borrowed from the New Legislative Framework, with essential requirements and a presumption of conformity based on harmonised standards (Chiara, 2025). Article 27 of the Cyber Resilience Act makes this connection concrete: products certified under a recognised scheme, such as the EUCC, benefit from that presumption (EPRS, 2026). Voluntary certification under the 2019 Act therefore becomes central to obligations that are mandatory under the Cyber Resilience Act. A certified operator can avoid duplicating assessments, which lowers administrative burden. But this also creates a risk: a scheme designed to be voluntary may become, in practice, close to compulsory for operators trying to cut compliance costs. Industry has flagged coordination problems since the Cyber Resilience Act was adopted, and these remain unresolved. The clearest example is the overlap between NIS2 obligations for cloud providers and Cyber Resilience Act obligations for remote data-processing solutions (DIGITALEUROPE, 2024, p. 20). The January 2026 revision, linked to a parallel proposal amending NIS2, seems aware of this problem (Covington & Burling, 2026). Still, it is not yet clear whether greater institutional complexity will bring real security gains or simply add another layer of compliance for small and medium-sized enterprises.

5. CONCLUSIONS

The analysis developed throughout this article confirms that the ongoing revision of Regulation (EU) 2019/881 should not be understood as reflecting the emergence of a new autonomous Union competence in the field of cybersecurity. Rather, it demonstrates the continuing capacity of the competences conferred upon the Union by the Member States—most notably under Article 114 TFEU—to accommodate increasingly complex technological developments through progressively more sophisticated techniques of internal-market harmonisation. While the technological, economic and strategic environment has evolved profoundly since the adoption of Regulation (EU) 2019/881, the legal rationale underpinning Union action has remained substantially unchanged. What has evolved is not the distribution of competences established by the Treaties, but the regulatory techniques through which the Union pursues the objectives entrusted to it by the Member States.

Against this broader legal background, taken together with the internal-market dimension discussed in the earlier part of this contribution, the substantive-security and strategic dimensions examined here point to one clear conclusion: the Cybersecurity Act cannot be reduced to either

technical harmonisation law or security law alone. Regulation (EU) 2019/881, together with the revision under way between 2025 and 2026, is best understood as a hybrid instrument. Certification operates at the same time as a tool for removing technical barriers to intra-European trade, as a way of turning security by design into positive law, and, increasingly, as a vehicle for strategic-autonomy ambitions that the internal-market toolkit was never built to carry. The Cyber Solidarity Act makes this tension explicit. It steps outside Article 114 TFEU altogether, yet still limits its own collective-response logic through non-affectation clauses that leave national security firmly in the hands of Member States (Villani, 2025). This is a useful reminder: whichever legal basis is chosen, EU cybersecurity law still operates at the edge of the Union's traditional security competences, rather than fully within them.

The so-called "Brussels effect" describes how EU digital regulation becomes a reference point for operators well beyond the Union's borders (Bradford, 2020). Here, this effect works in two directions. Towards the market, it works through the voluntary alignment of non-European manufacturers with European schemes. Towards security, it works through the export of risk-management standards, increasingly shaped by hybrid warfare threat perceptions and by the still unsettled question of when a cyber operation crosses the threshold into armed conflict or an act of war (Delerue, 2020; Kilovaty, 2022, p. 251). Whether this amounts to genuine resilience, to a coherent affirmation of EU digital sovereignty (Barrinha & Christou, 2022), or simply to a further layer of regulatory complexity is not yet clear. The answer will depend less on the final text of the 2026 negotiations than on something more practical: whether EU institutions, ENISA above all, can secure resources that match a mandate which, as the Commission itself admits, has grown faster than the operational capacity needed to deliver it. Ultimately, the future development of European cybersecurity law will depend not upon the creation of new Union competences, but upon the continuing ability of the existing legal framework to reconcile internal-market integration, technological innovation and increasingly complex cybersecurity objectives within the limits established by the Treaties.

REFERENCES

1. Barrinha, A., & Christou, G. (2022). Speaking sovereignty: The EU in the cyber domain. *European Security*, 31, 356.
2. Bird & Bird. (2026, January). *The EU Cybersecurity Act.* https://www.twobirds.com/en/capabilities/practices/digital-rights-and-assets/european-digital-strategy-developments/cybersecurity/cybersecurity/the-eu-cybersecurity-act
3. Bradford, A. (2020). *The Brussels effect: How the European Union rules the world.* Oxford University Press.
4. Brighi, R., & Chiara, P. G. (2021). La cybersecurity come bene pubblico: alcune riflessioni normative a partire dai recenti sviluppi nel diritto dell'Unione Europea [Cybersecurity as a public good: Some regulatory reflections following recent developments in EU law]. *Federalismi.it*, 21, 18-42.
5. Bygrave, L. A. (2021). Security by design: Aspirations and realities in a regulatory context. *Oslo Law Review*, 8, 126.
6. Chiara, P. G. (2022a). The Cyber Resilience Act: The EU Commission's Proposal for a Horizontal Regulation on Cybersecurity for Products with Digital Elements: An Introduction. *International Cybersecurity Law Review*, 3(2), 255–272.
7. Chiara, P. G. (2022b). The IoT and the new EU cybersecurity regulatory landscape. *International Review of Law, Computers & Technology*, 36, 118, 130–131.
8. Chiara, P. G. (2025). Understanding the regulatory approach of the Cyber Resilience Act: Protection of fundamental rights in disguise? *European Journal of Risk Regulation*, 16(2), 469–484. https://doi.org/10.1017/err.2025.9
9. Coco, A., Dias, T., & van Benthem, T. (2022). Illegal: The SolarWinds hack under international law. *European Journal of International Law*, 33(4), 1275–1286. https://doi.org/10.1093/ejil/chac063
10. Covington & Burling. (2026, January 23). European Commission proposes Cybersecurity Act 2: New EU supply chain rules and certification reforms. *Global Policy Watch.* https://www.globalpolicywatch.com/2026/01/european-commission-proposes-cybersecurity-act-2-new-eu-supply-chain-rules-and-certification-reforms/
11. De Gregorio, G., & Dunn, P. (2022). The European risk-based approaches: Connecting constitutional dots in the digital age. *Common Market Law Review*, 59, 473.

12. Delerue, F. (2020). *Cyber operations and international law*. Cambridge University Press.
13. Digital Watch Observatory. (2026, January 19). EU revises Cybersecurity Act to streamline certification. https://dig.watch/updates/cybersecurity-act-enisa-eu-certification-review
14. DIGITALEUROPE. (2024). *The single market love story: 10 digital actions to save the 30-year marriage* (p. 20). https://cdn.digitaleurope.org/uploads/2024/02/DIGITAL-EUROPE-THE-SINGLE-MARKET-LOVE-STORY-FINAL-WEB.pdf
15. Engel, A. (2025). Licence to Regulate: Article 114 TFEU as Choice of Legal Basis in the Digital Single Market. In A. Engel, X. Groussot, & G. T. Petursson (Eds.), *New Directions in Digitalisation: Perspectives from EU Competition Law and the Charter of Fundamental Rights* (pp. 13–28). Cham.
16. European Council on Foreign Relations. (2025). *Alone we stand: How Europe can counter hybrid threats in a post-transatlantic era.* https://ecfr.eu/article/alone-we-stand-how-europe-can-counter-hybrid-threats-in-a-post-transatlantic-era/
17. European Parliamentary Research Service. (2026, January). *Cybersecurity Act review: What to expect* [At a Glance]. https://epthinktank.eu/2026/01/05/cybersecurity-act-review-what-to-expect/
18. Farrand, B., Carrapico, H., & Turobov, A. (2024). The new geopolitics of EU cybersecurity: Security, economy and sovereignty. *International Affairs*, 100(6), 2379–2397. https://doi.org/10.1093/ia/iiae231
19. Finocchiaro, G. (2023). *Diritto di Internet* [Internet law] (4th ed.). Zanichelli.
20. González Fuster, G., & Jasmontaite, L. (2020). Cybersecurity Regulation in the European Union: The Digital, the Critical and Fundamental Rights. In M. Christen, B. Gordijn, & M. Loi (Eds.), *The Ethics of Cybersecurity* (pp. 97–115). Cham.
21. Kilovaty, I. (2022). Cyber conflict and the thresholds of war. In D. L. Sloss (Ed.), *Is the international legal order unraveling?* (p. 251). Oxford University Press.
22. Lotito A., Dalli H. (2026), *Digital Package – Revision of the Cybersecurity Act: Implementation Takeaways*, European Parliamentary Research Service (EPRS), European Parliament, PE 774.675 (1-11).
23. Palmieri, N. (2026, January). EU Commission proposed new Cybersecurity Act. *Baker Botts.*

https://ourtake.bakerbotts.com/post/102m2iw/eu-commission-proposed-new-cybersecurity-act
24. Stewart Ferguson, D. D. S. (2022). European Cybersecurity Certification Schemes and Cybersecurity in the EU Internal Market. *International Cybersecurity Law Review*, 3(1), 51–114.
25. Taddeo, M. (2019). Is cybersecurity a public good? *Minds and Machines*, 29, 349, 351.
26. Vallejo, R. (2021). The Private Administrative Law of Technical Standardization. *Yearbook of European Law*, 40, 172–229.
27. Varju, M. (2020). 5G networks, (cyber)security harmonisation and the internal market: The limits of Article 114 TFEU. *European Law Review*, 471.
28. Villani, S. (2025). The Cyber Solidarity Act: Framework and perspectives for the new EU-wide cybersecurity solidarity mechanism under the EU legal system. *European Journal of Risk Regulation*, 16(2), 485–497.
29. **EU Legislation and Policy Documents**
30. Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency.
31. 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, 7.6.2019.
32. European Commission, *A European Strategy for Data*, COM(2020) 66 final, Brussels, 19.2.2020.
33. European Commission, *Shaping Europe's Digital Future*, COM(2020) 67 final, Brussels, 19.2.2020.
34. European Commission, *2030 Digital Compass: The European Way for the Digital Decade*, COM(2021) 118 final, Brussels, 9.3.2021.
35. Decision (EU) 2022/2481 of the European Parliament and of the Council of 14 December 2022 establishing the Digital Decade Policy Programme 2030, OJ L 323, 19.12.2022.
36. 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 L 333, 27.12.2022.

37. Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011, OJ L 333, 27.12.2022.
38. Commission Implementing Regulation (EU) 2024/482 of 31 January 2024 adopting the European Common Criteria-based Cybersecurity Certification Scheme (EUCC), OJ L, 2024/482, 7.2.2024.
39. 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, 20.11.2024.
40. Commission Implementing Regulation (EU) 2024/3143 of 18 December 2024 on notifications under Article 61(5) of Regulation (EU) 2019/881, OJ L, 2024/3143, 19.12.2024.
41. Regulation (EU) 2025/37 of the European Parliament and of the Council of 19 December 2024 amending Regulation (EU) 2019/881 as regards managed security services, OJ L, 2025/37, 15.1.2025.
42. 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 (Cyber Solidarity Act), OJ L, 2025/38, 15.1.2025.
43. European Commission, *Proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Cybersecurity (ENISA), the European cybersecurity certification framework, and ICT supply chain security and repealing Regulation (EU) 2019/881 (The Cybersecurity Act 2)*, COM(2026) 11 final, Strasbourg, 20.1.2026.

Case Law

1. Court of Justice, 5 October 2000, Case C-376/98, *Germany v Parliament and Council*, ECLI:EU:C:2000:544.
2. Court of Justice, 10 December 2002, Case C-491/01, *British American Tobacco*, ECLI:EU:C:2002:741.
3. Court of Justice, 8 June 2010, Case C-58/08, *Vodafone and Others*, ECLI:EU:C:2010:321.