# EU – US COMPARISON OF APPROACHES TO CYBERSECURITY CERTIFICATION AND STANDARDIZATION

Václav Stupka/ Jakub Vostoupal / Pavel Loutocký

Václav Stupka, PhD, postdoc researcher; Masaryk University, Faculty of Informatics, Faculty of Law, Institute of Law and Technology; Žerotínovo nám. 617/9, 601 77 Brno, CZ; e-mail: vaclav.stupka@law.muni.cz;

Jakub Vostoupal, researcher, Masaryk University, Faculty of Informatics; Botanická 68a, Brno, CZ; e-mail: Jakub.vostoupal@law.muni.cz

Pavel Loutocký, PhD, postdoc researcher; Masaryk University, Faculty of Informatics, Faculty of Law, Institute of Law and Technology; Žerotínovo nám. 617/9, 601 77 Brno, CZ; e-mail: loutocky@muni.cz;

***Keywords:*** ***cybersecurity standardization, cybersecurity certification, cybersecurity act, cyber resilience act, comparative law***

***Abstract:*** *The increasing dependence of the information society on the confidentiality, availability and integrity of information and communication systems is forcing countries to introduce regulations to protect key infrastructures and systems. One of the tools of this regulation is the standardization and certification of ICT products and services. This area has undergone dynamic development in recent years, both in terms of the method of regulation and the approach to defining security requirements. This paper compares approaches to cybersecurity standardization and certification in the US and the EU, particularly in the context of new and pending legislation in the EU in the form of the Cybersecurity Act and the forthcoming Cyber Resilience Act. The paper aims to identify the differences between these regimes and their compatibility from the perspectives of certification providers, vendors and users.*

## 1. Introduction[1]

Cybersecurity regulation is often based on so-called performance-based rules. Rather than specifying the actions regulated entities must take, performance-based regulation instead requires the attainment of outcomes and gives flexibility in how to meet them[2]. This approach is particularly advantageous in technological areas and especially in cybersecurity, as it allows the regulation to be technology-neutral and allows regulated entities to choose the appropriate tools and measures to ensure a sufficient level of security that is cost-effective and appropriate in relation to the conditions of the operator, the type of infrastructure operated and the technologies used. However, this regulatory method cannot be considered a silver bullet, as it introduces entirely new problems.

One of these problems is limited legal certainty on the part of both the regulated entity and the regulator or supervisory authorities. Regulators, who are generally accustomed to enforcing relatively well-defined prescriptive rules, are not accustomed to being held accountable for enforcing loosely formulated performative rules. This is especially true when performance cannot be objectively measured, evaluated and verified. In such a

[1] This article is a result of a research project no. VJ01030007 Standards in cybersecurity, which was supported by the Ministry of interior of the Czech Republic in a project scheme Strategic support of the security research 2019–2025 (IMPAKT-1). This article expresses opinions of the authors and the project team, these are not the opinions of the institutions the authors represent nor the Ministry of interior.

[2] For more on performance based regulation please see i.e. Coglianese C., The Limits of Performance-Based Regulation, 50 U. Mich. J. L. Reform 525 (2017). Available at: https://repository.law.umich.edu/mjlr/vol50/iss3/1.

case, a high degree of discretion is placed in the hands of the regulator, for which the regulator is responsible and which may, at the same time, be subject to abuse. Regulated entities may then feel uncomfortable with loosely formulated performative rules, as they are not assured that the chosen methods and tools of compliance will be considered appropriate and sufficient by the regulator[3].

The general goal is thus to reduce the uncertainty arising from the use of performative rules as much as possible. The obvious way is to set sufficiently clear rules and specific metrics for assessing compliance. However, these ex-ante measures may not be applicable in rapidly changing areas of regulation, such as cybersecurity. In these cases, ex-post uncertainty reduction tools can then be considered. Such tools are, for example, standardization and certification. This article compares the approach to the use of these mechanisms for increasing legal certainty in the field of cybersecurity in two entirely different legal cultures – the US, where the emphasis is on ex-post oversight to promote innovation; and the EU, where there is a marked drive towards ex-ante regulation to ensure a high level of protection of fundamental rights and freedoms[4]. These two approaches then have clear implications for how standardization and certification are applied in relation to performative rules.

## 2. Frameworks, standards and certification in cybersecurity

Standards can be understood as specifications used to achieve maximum functionality, purpose, reliability, safety or efficiency of a product, service or infrastructure. Standards are usually formulated as documentation that defines the specifications, processes, and procedures to be applied to achieve these objectives. Standards reflect the general consensus of the professional community and are validated by some legal entity – public or private authority[5]. On standards are then built certification systems that allow independent verification of the conformity of the relevant products, services or processes with the chosen standard. The conformity assessment body and the certification laboratory assess conformity to the defined standard through predefined procedures and verify the achievement of the specified criteria. Certification can then be obtained by product manufacturers, service providers, or infrastructure operators voluntarily for, i.e. compliance or competitive advantage, or on a mandatory basis if required by related legislation or customer. However, compliance with the standard can also be declared directly by the manufacturer, provider or operator without independent verification through a self-assessment and subsequent issuance of a declaration of conformity. The use of standards can then be supported from below by frameworks. While standards explain and provide methods one by one, specify what is expected to be done to complete the process, and clarify methods to coincide with the standard, a framework is a general guideline that covers many components or domains that can be adopted by businesses/companies/institutions, which does not specify the steps that are required to be taken[6].

All these mechanisms are now also applied to varying degrees in the field of cybersecurity, essentially worldwide. However, they differ significantly in which mechanism they favour and how they aim to enhance legal certainty. There is a spectrum of cybersecurity regulatory frameworks worldwide, ranging from more government-centric approaches to voluntary initiatives. The government-centric approach focuses on topdown, ex-ante tendencies where regulators define relatively precise rules and require regulated entities to verifiably

[3] For more on stakeholders view of performative rules and standards, please see Performance-Based Regulation: Prospects and Limitations in Health, Safety, and Environmental Protection," Regulatory Policy Program Report No. RPP-03 (2002).

[4] For more on comparison of ex-ante and ex-post regulation please see i.e. FRIEDEN, Rob. Ex Ante Versus Ex Post Approaches to Network Neutrality: A Comparative Assessment. Berkeley Technology Law Journal. 2015, 30(2), 52. Available at: doi:10.15779/Z386Z81

[5] See i.e. Karie, N.M.; Sahri, N.M.; Yang, W.; Valli, C.; Kebande, V.R. A Review of Security Standards and Frameworks for IoT-Based Smart Environments. IEEE Access 2021, 9, 121975–121995.

[6] See Seeburn, K. Basic Foundational Concepts Student Book: Using COBIT® 5; ISACA: Schaumburg, IL, USA, 2014. and Taherdoost, H. Understanding Cybersecurity Frameworks and Information Security Standards–A Review and Comprehensive Overview. Electronics 2022, 11, 2181. https://doi.org/ 10.3390/electronics11142181.

submit to these rules, which can be achieved through mandatory certification. Voluntary initiatives focus on bottom-up development of guidelines in the form of cybersecurity framework, which the regulated entities can voluntarily follow to achieve compliance with binding performance-based rules that can be reviewed ex-ante by regulatory authorities. These are, however, two extremes, and most countries are somewhere in between. This paper thus compares the US and the EU approaches and their fundamental differences.

## 3. The US approach to cybersecurity regulation

Cybersecurity law can be defined as one that promotes the confidentiality, integrity, and availability of public and private information, systems, and networks, through the use of forward-looking regulations and incentives, with the goal of protecting individual rights and privacy, economic interests, and national security[7], is rather patchy scattered across multiple federal and state statutes, and common law claims. Specific regulation mainly deals with data security, data breach notification, data security litigation and electronic surveillance.

Data security is only regulated explicitly in some states, usually very generally as a part of corporate duediligence requirements and consumer protection. Federal oversight of data protection is carried out by the Federal Trade Commission as part of its fair market oversight. However, clear rules or parameters assessed in evaluating the level of data protection are not defined here either. Data protection is regulated explicitly in selected sectors, such as the healthcare or financial sectors. Data breach notification is not regulated at the federal level, but 48 states require notification to customers or regulators in their laws. However, the notification rules and parameters vary among states, creating a compliance challenge for corporate compliance for companies operating in multiple states. In general, however, the goal of notifications is to limit the negative impact of a data breach on customers.

A consequence of the common law nature of the US legal culture is the great importance of data security litigation, a powerful ex-post regulatory tool applied in class action lawsuits that arise from common law claims such as negligence, negligent misrepresentation, breach of contract, breach of an implied warranty, or unjust enrichment. The risk of lawsuits, in turn, indirectly motivates service providers to a higher level of cybersecurity in order to avoid potential legal liability. However, this motivation is directed towards ensuring only one component of cybersecurity – confidentiality, as it is only very rarely that lawsuits arise due to a lack of integrity or availability of services and data. Another piece of legislation that can be considered a kind of cybersecurity legislation is The Electronic Communications Privacy Act, which limits the ability not only of the government but also of electronic communications network operators to monitor telecommunications traffic. In addition, a critical specific cybersecurity regulation in the US is the Cybersecurity Act of 2015[8], which primarily builds tools for public-private cooperation. This regulation allows private entities to monitor their information systems to ensure cybersecurity, to use "defensive measures" to ensure cybersecurity and share information on cybersecurity indicators and defensive measures with other private entities and public authorities. Thus, the US Cybersecurity Act essentially builds mechanisms for cooperation and provides limited protection from liability that may arise in connection with monitoring infrastructures, sharing cybersecurity information, and using defensive measures. However, it does not seek to oblige regulated entities to apply any preventive cybersecurity measures or tools. Finally, there are two additional relevant federal statutes – the National Cybersecurity and Critical Infrastructure Protection Act of 2013 that codifies the role of the US Department of homeland security (DHS) in preventing and responding to cyber security incidents and establishes an information-sharing partnership between DHS and the owners and operators of the critical infrastructure

[7] See Kosseft, J., Defining Cybersecurity Law, 103 Iowa Law Review. 985 (2018). Available at: https://ilr.law.uiowa.edu/assets/Uploads/ILR-103-3-Kosseff.pdf.

[8] Online available at: Cybersecurity Act of 2015. https://www.intelligence.senate.gov/sites/default/files/legislation/Cybersecurity-Act-Of-2015.pdf. For detailed analysis of the act please see i.e. Tran, Jasper L. Navigating the Cybersecurity Act of 2015. Chap. L. Rev., 2016, 19: 483.

and the Cybersecurity Enhancement Act that gives the National Institute of Standards and Technology (NIST) the authorization and support to develop voluntary standards to reduce the risk of cyberattacks to critical infrastructure[9].

As can be seen from the preceding text, cybersecurity legislation in the US is relatively general and leaves much room for interpretation, and obligated persons are motivated to implement cybersecurity measures primarily by liability risk and economic and reputational motivators. Thus, supporting mechanisms to ensure compliance and narrow the scope for liability are vital. NIST is a crucial institution in this area since it develops standards and frameworks based on the aforementioned statutes, executive orders and policies. The primary resource developed by NIST is the Cybersecurity Framework[10], which is voluntary guidance based on existing standards, guidelines, and practices for organizations to better manage and reduce cybersecurity risk. The Cybersecurity Framework consists of three main components: (i) the Core, which guides organizations in managing and reducing their cybersecurity risks; (ii) the Implementation Tiers, that guide organizations to consider the appropriate level of rigor for their cybersecurity program; and (iii) the Profiles, that enable organizations to establish a roadmap for reducing cybersecurity risk that is well aligned with organizational and sector goals, considers legal/regulatory requirements and industry best practices, and reflects risk management priorities[11]. In addition, the framework links to other frameworks (such as the Privacy Framework[12] or the Risk Management Framework[13]) and especially individual standards related to specific security parameters, technologies, or processes. The implementation of frameworks and standards is also supported by the activities of the NICE National Cybersecurity Centre of Excellence[14], which implements projects in which it practically implements standards on a specific technology, cybersecurity challenge or in a specific sector, documents the whole process and subsequently publishes non-binding security guidance describing how compliance with the relevant standards can be achieved. All of these activities are carried out by NIST in close collaboration with industry, ensuring that current practices, state-of-the-art technology and industry standards are considered. There is also non-binding Common Criteria certification in the US, carried out by conformity assessment bodies and certification laboratories accredited by the National Institute of Standards and Technology under the National Voluntary Laboratory Accreditation Program.

Thus, in the US, the rules for cybersecurity of products, services and infrastructures are defined in the private sphere in relatively general terms, relying primarily on the internal and external motivation of the organizations themselves to follow existing standards, which are primarily voluntary. Compliance with standards or even certification is only required in selected cases, for example, in the context of critical infrastructure or government information and communication systems. At the same time, however, clear and effective support for the implementation of standards is provided to the application community by public institutions (i.e. NIST). As a result, responsibility for security is left more in the hands of the application domain and relies more on ex-post verification in the context of litigation. This provides more room for innovation but also potentially increases the level of risk to consumer and public liberty rights. However, no data or research outputs are available that objectively measure or assess the practical impact of this approach on safety or innovation.

9 See Pernik, P., Wojtkowiak, J. and Verschoor-Kirss, A. National Cyber Security Organisation: UNITED STATES. Talinn: NATO Cooperative Cyber Defence Centre of Excellence, 2016. Available at: https://www.ccdcoe.org/uploads/2018/10/CS_organisation_USA_122015.pdf.

10 See online at: https://www.nist.gov/cyberframework/framework-documents.

11 Individual profiles are described online here: https://www.nist.gov/cyberframework/examples-framework-profiles.

12 For more see online here: https://www.nist.gov/privacy-framework.

13 For more see online here: https://csrc.nist.gov/Projects/risk-management.

14 Online here: https://www.nccoe.nist.gov.

## 4. The EU approach to cybersecurity regulation

The approach of the EU to cybersecurity differs significantly from the US for two main reasons. The first is the different legal culture, as the US system is governed by the Common Law traditions, which are necessarily bound to be more flexible and the fact that there is far more experience with performance-based regulation in the US legal culture. In contrast, the EU is governed mainly by the traditions of Civil Law, which are prone to be more rigid and strict in regulation. The second reason is the relative lack of experience with the cybersecurity regulation and cybersecurity market on the EU part. The US has tried several different approaches to cybersecurity regulations, but in the end, decided to leave much room for the cybersecurity market to self-regulate and not interfere as much with the standardization and certification regulations (even though there is still quite a lot of interference in the area of, e.g., water services).[15] The resulting effect is that the cybersecurity market in the US is much more independent, self-sufficient (as it already has a relatively great deal of experience), encouraging innovations, and open to lobbying; however, it is also challenging to regulate when security measures are needed.[16]

Were the cybersecurity market of the EU opened in such a way, it would probably result in a great deal of chaos, uncertainty and market failure, mainly because of the lack of experience. Thus, the EU environment is more suitable for the more strict, top-down regulations approach.[17]

The beginnings of the EU cybersecurity regulations were relatively slow and timid. The EU made almost no attempts to regulate the cybersecurity field until 2004, when the ENISA was founded by Regulation (EC) No 460/2004[18]. However, it was the year 2013 and the introduction of the draft of the NIS Directive[19]that marked the actual change. Since then, the EU has introduced several regulatory acts and proposals relating to standardization and certification procedures in the cybersecurity field. The NIS 2 Directive proposal[20], the Cybersecurity Act[21] and the new Cyber Resilience Act proposal (CRA)[22] are probably the most important.

While the NIS 1 and NIS 2 Directives are both based on performative rules, the NIS 1 Directive did not entail any noteworthy mentions of the cybersecurity certification procedures nor of using any relevant standards, both being efficient compliance procedures that solve the uncertainty of the performative rules. However, it is essential to note that the NIS 1 Directive was the first major regulation that brought cybersecurity to the attention of many Member states for the first time. As the certification procedures were relatively advanced matter and poorly known among most of the EU at that time, they were not included and instead introduced in the Cybersecurity Act. The same could be said for the matter of European cybersecurity standardization, which was mainly in the hands of the private sector.

With a bit of simplification, European Standardization is generally not that different from the US system, even though it is still a product of supranational cooperation. The main initiatives are the product of private sector initiatives (the creation of standards is usually initiated by the stakeholders as opposed to the European certification system, see below), and its main objective "*is to agree on common specifications and/or proce-*

15 Bellantuono, G. Comparing Smart Grid Policies in the USA and EU. Law, Innovation and Technology. 2014, no. 2, pp. 231–235.

16 Ibid.

17 Ibid., pp. 233–240.

18 The 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

19 Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

20 Introduced on 16th December 2020. The legislation is still in progress as of the day of writing this article.

21 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

22 The proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020. Introduced on 15th September 2022. The legislation is still in progress as of the day of writing this article.

*dures that respond to the needs of business and meet consumer expectations* "[23]. It is mainly a voluntary way of sharing standardized best practices and consolidating the environment of the Single Market, as well as strengthening the European competitiveness and facilitation of cross-border trade, as the European standards are an efficient way to unite the Single Market (one European Standard effectively replaces up to 34 national standards that could be in conflict).[24] Moreover, many private entities use standards to sufficiently uphold and comply with relevant legislation.[25] However, even though the Union recognizes primary standardization associations (CEN, CENELEC and ETSI[26]) as the European Standardization Organizations and ENISA promotes greater cooperation with these entities, the activities of European Standardization Organizations are not so heavily regulated[27] – e.g., the Commission does not dictate what standards should be made. Therefore, it is possible to view standards as a sort of horizontal initiatives and cooperations of the market and relevant stakeholders, as opposed to the European certification system, which is based on vertical regulation by the Commission and ENISA.

The story of the European certification is slightly different. It should be noted that the European "certification landscape" was moulded for a long time by a long-standing lack of knowledge, political interest, and capacities in the cybersecurity industry. Thus, in the past, only a few Member States[28] had taken an interest in the certification procedures for the cybersecurity of technologies and the primary source of experience even for those States was the international certification system of Common Criteria.[29],[30] However, the nature of cooperation among the Member States proved to be an advantage in this field and led to the creation of a group called SOG-IS[31], which is a collective of 14 Member States and Norway cooperating more closely than others, who were operating under the regime of Common Criteria.[32] As a result, the SOG-IS group proved to be an efficient way of producing more certification schemes (or rather protection profiles) in a much faster way, and also the only way to internationally (or rather only among the SOG-IS members) recognize certificates up to the fourth security level (in comparison with the second level under the Common Criteria)[33].[34] Because of many problems that haunted the Common Criteria system[35], the certificatory giants felt the need for another system that would suit their needs, specifically one that would be more flexible, offer lower security levels,

---

23 European Standardization [online]. *CEN-CENELEC*. 2022 [accessed 30. 11. 2022]. https://www.cencenelec.eu/european-standardization/

24 Ibid.

25 Ibid.

26 CEN is the European Committee for Standardization, CENELEC the European Electrotechnical Committee for Standardization, ETSI the European Telecommunications Standards Institute. CEN and CENELEC are international non-profit associations bringing together national standardization bodies.

27 Partly because standards are primarily only voluntary ways of achieving compliance.

28 Mainly France, Germany, and Netherlands. Until the Brexit, even the UK was considered one of the EU certificatory giants. The rest of the SOG-IS collective had also relevant capacities, even though somewhat limited in comparison with the "giants" (the equipping and running of a certification authority and testing laboratory is very demanding business). It was also not uncommon that the Member State had no relevant knowledge, legislation and capacities whatsoever (e.g., Czechia).

29 Common Criteria [online]. New CC Portal [accessed 25. 10. 2022]. https://www.commoncriteriaportal.org/

30 For more information about the Common Criteria system, see inter alia Tantawi, R. Common Criteria. *Salem Press Encyclopedia*. 2013. https://eds.a.ebscohost.com/eds/detail/detail?vid=1&sid=65cb00d8-2765-434e-802f-29a488b6180b%40sdc-v-sessmgr04&bdata=JkF1dGhUeXBlPWlwLGNvb2tpZSx1aWQmbGFuZz1jcyZzaXRlPWVkcy1saXZlJnNjb3BlPXNpdGU%3d#db=ers&AN=90558266

31 The SOG-IS Group was created based on Council Decision 92/242/EEC of 31st March 1992 on the security of information systems and Council Recommendation 1995/144/EC of 7th April 1995 on general criteria for assessing the security of information systems.

32 SOG-IS – Status of participants [online]. SOG-IS [accessed 25. 10. 2022]. http://sogis.org/uk/status_participant_en.html

33 The maximum-security level is seven. However, only the first four levels can be assessed in the international testing laboratories, as the methodology for the higher levels is missing. The reason for this is the lack of mutual trust about rigor and expertise of testing capabilities of other members of Common Criteria. Thus, the US demanded, that the highest security levels should be tested only in their own laboratories.

34 Mitrakas, A. The emerging EU framework on cybersecurity certification. Datenschutz und Datensicherheit. 2018, no. 7.

35 Mainly the slow creation of up-to-date protection profiles and schemes, rigorous lengthy and costly procedures (even for the low security/assurance levels) and problems with recertification, patches and services. For more, see inter alia Kallberg, J. The Common Criteria Meets Realpolitik: Trust, Alliances, and Potential Betrayal. *IEEE Security & Privacy Magazine*. 2012, no. 4.

have a faster certification procedure and be much cheaper. Unfortunately, despite all its benefits, SOG-IS cooperation could not sufficiently meet these needs as it was still bound by the Common Criteria requirements and core documents. The frustration, caused not only by the inefficient system but also by the mandatory testing of high-level-security technologies in the US (which presented a potential national security risk),[36] rose so high that the idea of universal recognition of certificates was once more abandoned. The EU certification market fractured into a plethora of unique national and industry-based schemes and many internal standards. It is thus unsurprising that the number of different certificates circulating in the EU is immeasurable.[37] This fragmentation of the market creates an absurd situation where a manufacturer who wants to sell his product in France, Germany and the Netherlands has to have his product certified according to the "*Certification Cécuritaire de Premier Niveau* " in France, the "*Baseline Product Assessment*" in the Netherlands and a specially adapted Common Criteria model in Germany (the so-called "*German Certificate* "). They are thus forced to undergo three (still) lengthy and costly procedures, presenting many manufacturers with an obstacle they are unwilling or unable to overcome.[38] This is a grotesque mockery of the European idea of the single digital market, which is unreachable without a firm cybersecurity and at least a sound cybersecurity certification strategy (primarily because of public procurement).[39] It was also apparent that the Member States could not reach a deeper understanding and consensus to mitigate this situation.[40]

## 5. The Cybersecurity Act

Because the cybersecurity market of the EU was shattered by numerous national certification systems and different internationally unrecognizable obligations, the need for change was evident. Thus came the Cybersecurity Act. The Cybersecurity Act has two core parts: first, it changes the way ENISA functions and gives it a permanent mandate, more funds, capacities and also obligations. The second, more revolutionary part is creating a certificatory framework for a system that might eclipse even the Common Criteria – certification procedures for cybersecurity aspects of products, services and processes with certificates universally recognized across the EU.[41] Through the methodology and tools of this framework, the EU can create its own certification schemes, which would unite the EU cybersecurity market because such schemes would effectively replace their national variants.[42] Each scheme shall be focused on a different technology (cloud services, 5G technologies, IoT etc.). The first scheme in preparation is the EUCC – a certification scheme that shall incorporate the Common Criteria system into the EU certification framework. The preparation of schemes was mainly entrusted to ENISA.[43]

One of the cornerstones of the whole certification framework is the so-called conformity assessment bodies, the certification authorities, which administer the certification process and cooperate with testing laboratories.[44] The requirements prescribed by the Cybersecurity Act on these bodies are far from lenient, and there is a great interest in creating these bodies throughout the EU as the potential monopoly of the certification "gi-

36 This obligation rose from the Common Criteria core documentation and Methodology. See Arrangement on the Recognition of Common Criteria Certificates In the field of Information Technology Security – Ratification on the 8th September 2014. 2014. https://www.commoncriteriaportal.org/files/CCRA%20-%20July%202,%202014%20-%20Ratified%20September%208%202014.pdf

37 Drogkaris, P. Considerations on ICT security certification in EU – Survey Report. European Union Agency for Network and Information Security, 2017. https://www.enisa.europa.eu/publications/certification_survey/at_download/fullReport

38 Negreiro Achiaga, M. D. M. EU Legislation in Progress – Briefing: ENISA and a new Cybersecurity Act (as of 16 January 2018). European Parliament Research Service, 2018. http://www.europarl.europa.eu/RegData/etudes/BRIE/2017/614643/EPRS_BRI(2017)614643_EN.pdf

39 Ježová, D. EU Digital Single Market – Are we there yet? Ad Alta: Journal of Interdisciplinary Research. 2017, no. 2, pp. 99–100.

40 Commission Staff Working Document – Summary of the Impact Assessment on the draft of the Cybersecurity Act. European Commission, 2017. https://eur-lex.europa.eu/legalcontent/CS/TXT/HTML/?uri=CELEX:52017SC0501&from=CS

41 See Article 56 of the Cybersecurity Act.

42 See Article 57 of the Cybersecurity Act.

43 See Article 49 of the Cybersecurity Act. During the scheme-preparation phase ENISA should cooperate with all relevant stakeholders, including European Standardization Organizations.

44 See Article 60 of the Cybersecurity Act.

ants" could be devastating for the single digital market. However, the missing accreditation schemes, which (basically) tell the conformity assessment body what capacities are needed to perform the certification and be accredited as a certification-capable body, effectively prevent this from happening. These schemes should have been part of the certification schemes, and even though the draft schemes for the EUCC and cloud services are available, the lack of accreditation schemes prevents the creation of entirely new conformance assessment bodies (such as is the case in the Czechia).[45]

## 6. The Winds of Change

Even though the cybersecurity certification under the Cybersecurity Act was prepared initially as generally voluntary and only obligatory where a Member State or Commission would deem otherwise[46], the proposals for the NIS 2 Directive and CRA might severely affect this, as the EU is potentially tightening the grip on the general level of cybersecurity in the single digital market.

The NIS 2 Directive specifically mentions using European cybersecurity certification schemes in Article 21 to demonstrate compliance with cybersecurity risk management measures laid down in Article 18. This may even be made obligatory for specific entities (essential or important entities under the NIS 2 Directive) either by the will of the Commission or the Member States.[47] Furthermore, the same article propagates the usage of certified products, services and processes in the areas where the Commission identifies insufficient levels of cybersecurity and deeply incorporates certification into the new EU cybersecurity ecosystem.[48] In order to further and more effectively implement the new cybersecurity risk management measures of Article 18, the NIS 2 Directive also encourages the use of relevant European or internationally accepted standards and specifications, as well as deeper cooperation between ENISA, Member States and relevant standardization stakeholders.[49] Even so, it is evident that certification is the primary focus of public regulation, and standardization still remains more in the hands of the private sector.

The Cyber Resilience Act is focused on improving the cybersecurity of products with digital elements in more of a horizontal way, even though the European certification schemes are still mentioned multiple times throughout the Act. The CRA propagates the certifications and self-assessment procedures quite heavily as a way of conformance demonstration and a way of improving security even for low-level entities (not only those who are essential or important entities, according to the NIS 2 Directive).[50] Therefore, it can be expected that the importance of certification procedures and the number of regulations and obligations shall only rise. It is probable that once the certification framework is fully prepared and the CRA and NIS 2 Directive are in effect, more cybersecurity certification procedures will be obligatory.

## 7. Fundamental differences

As seen from the above analyses, the approach to cybersecurity standardization and certification in the US and the EU is fundamentally different in many respects. These differences stem from, among other things, the differences in the two legal cultures, different historical experiences and knowledge, and different levels of experience in cooperating with industry.

---

45 To further delve into the matter of the Cybersecurity Act, see e.g., Vostoupal, J. The Future of the Certification of Cybersecurity Technologies. Jusletter IT. Die Zeitschrift für IT und Recht. Weblaw, 2020, 30. September, s. 527–532. ISSN 1664-848X. doi:10.38023/7352d0dd-e589-420b-abd5-d7c03e3dfe6c

46 See Article 56 of the Cybersecurity Act.

47 See Article 21 of the Proposal for the NIS 2 Directive.

48 See Article 21, par. 2 and 3 of the Proposal for the NIS 2 Directive.

49 See Article 22 of the Proposal for the NIS 2 Directive.

50 See for example Article 24 of the Proposal for the Cyber Resilience Act.

The first key difference is evident in the level of intensity and detail of regulation. For the most part, both regions base regulation on the use of performative rules to achieve sufficient freedom and technological neutrality. However, while the US regulation is far vaguer and relies more on market support through non-binding frameworks and standards and its own ability to self-regulate, the EU is more rigid, and the level of specificity and detail of the performative rules formulated is significantly higher. The bottom-up approach of greater discretion of regulated sub-units and a greater degree of trust in market mechanisms is evident in the US. Although industry and the application sector are heavily involved in the process of formulating rules and setting standards and certification rules on cybersecurity in the EU as well, the regulator plays a major role in their final formulation, so there is a greater emphasis on a top-down approach to regulation.

Another key difference lies in the different approach to when and how regulatory intervention should primarily occur. The EU relies more on ex-ante regulation, consisting of setting up preventive regulatory and supervisory mechanisms, which is reflected, among other things, in a greater emphasis on the importance of certification. The US, on the other hand, gives a lot of leeway to the market in order to foster innovation through less exante regulation and more reliance on ex-post assessment of compliance in litigation and sanction mechanisms. Here again, there is a clear difference in legal cultures, with the EU giving more importance to the prevention of consequences for fundamental rights and freedoms and the US giving more leeway to the market in order to foster innovation and competitiveness.

Related to the previous two differences is the extent to which cybersecurity rules are formulated as voluntary or mandatory. The US legislation is primarily aimed at limiting liability in order to create mechanisms for cooperation and coordination of incident response, while mandatory rules, mandatory compliance with standards or certification are mainly applied to key government and critical information infrastructure, or in specific sectors and areas of regulation (for example, to ensure privacy protection). The EU imposes far more specific obligations and requirements, whether it is mandatory implementation of preventive security measures, detection mechanisms or notification, and increasingly so in non-critical infrastructures. At the same time, there is a much greater emphasis on certification mechanisms, which are designed to be voluntary, but it is an open secret that they will increasingly be applied as a mandatory requirement for entry into certain parts of the market.

Currently, there is not enough experience, data and research results to clearly indicate which of these approaches is better or more effective. It is clear that the EU approach will clearly provide a higher level of consumer, data, privacy and fundamental rights protection, but at the cost of reduced speed of innovation and competitiveness. The US, on the other hand, provides more freedom, which is good for the market, innovation and competitiveness, but at the cost of a higher risk of negative impacts on society and fundamental rights resulting from the effects of inadequate cybersecurity.

## 8. Conclusions

In this article, in addition to the basics of regulatory approaches, we have presented the importance and essence of certification in cybersecurity and its benefits for the whole field. We then went on to discuss the possible regulatory approaches and advancement to the issue, specifically elaborating on and comparing the possible approaches between the US and the EU perspectives.

As mentioned, it is not now possible to assess which attitude to the issue is more appropriate. These are both different methods to regulation overall and different experiences (of which the US has many more). It is therefore not possible to make a clear assessment of which approach is better, however, at least in the context of the approach taken in the EU, the more rigid set-up is proving problematic, particularly in the sense that although some schemes (particularly for conformity assessment bodies) should have been introduced already so that the market could be built up gradually, there are still delays and time lags in building up workable approaches to cybersecurity certification. The development in question is also not helped by the generally adopted approach of overregulation. Nevertheless, it may turn out that the de facto self-certification schemes embedded in the CRA can help to shift and increase market perception of the issue, at least in the initial stages.