

DOMINIK BIERECKI, CHRISTOPHE GAIE, MIROSŁAW KARPIUK,
JEAN LANGLOIS-BERTHELOT

The European Union and Digital Sovereignty: NIS 2 Directive, a Strategic Asset or Handicap in Geopolitical Cyberspace Competition?

Unia Europejska a suwerenność cyfrowa: dyrektywa NIS 2 – atut strategiczny czy obciążenie w geopolitycznej rywalizacji w cyberprzestrzeni?

Abstract

The global interconnection of cyberspace poses unprecedented challenges to the digital sovereignty of states and the extraterritorial application of their laws. This publication examines comparative legal frameworks and emerging cybersecurity norms, drawing on contemporary legal literature, in particular on analyses of extraterritorial jurisdiction in cyberspace. We will specifically analyze the requirements of the European Union's NIS 2 Directive and the complexities of its implementation. The central question is to what extent this directive, while seeking to strengthen the cyber resilience of Member States, could unintentionally constrain EU countries more than other major cyber powers, such as China and the United States.

The discussion will highlight the cyber risks inherent in this extraterritoriality of law, as identified by platforms like LawEdge, and examine the extraterritorial obligations of states in cybersecurity, as documented by initiatives such as EuRepoC. This article explores how, while necessary, the directive could paradoxically create competitive disadvantages for the EU. This study aims to provide an in-depth understanding of the tensions between national security imperatives, data protection, and the need for international cooperation in a borderless cyberspace, while emphasizing the practical implications for legal actors and businesses within the European Union and beyond.

KEYWORDS: NIS 2 Directive, cyberspace, cybersecurity, digital sovereignty.

SŁOWA KLUCZOWE: dyrektywa NIS 2, cyberprzestrzeń, cyberbezpieczeństwo, suwerenność cyfrowa.

DOMINIK BIERECKI – associate professor, Pomeranian University in Słupsk (Poland), e-mail: dominik.bierecki@upsl.edu.pl, ORCID – 0000-0001-6993-3974.

CHRISTOPHE GAIE – associate researcher, Laboratoire Magellan, Université Jean Moulin Lyon 3, French Prime Minister Services (France), e-mail: christophe.gaie@gmail.com, ORCID – 0000-0002-8252-5278.

MIROŚŁAW KARPIUK – full professor, University of Warmia and Mazury in Olsztyn (Poland), e-mail: mirosław.karpiuk@uwm.edu.pl, ORCID – 0000-0001-7012-8999.

JEAN LANGLOIS-BERTHELOT – head of the Division of Operational Sciences and Development, chair of teachings, Center for Advanced Military Training (France), e-mail: jeanlanglois4@gmail.com, ORCID – 0009-0001-2397-5930.

1 | Introduction

The democratization and rapid growth of internet usage have created an interconnected world, marked by the interdependence of information, economic activity, and development. Today, over 5.56 billion people – 67.9% of the global population – are active in cyberspace^[1], utilizing various internet-based services such as e-commerce, e-government, and more. However, this global digital interconnection also presents significant challenges to traditional notions of state sovereignty, which now extends into the digital realm. In this context, digital sovereignty refers to a state's ability to govern and control its digital infrastructure, data, and online activities by defining and regulating its national digital space.

The growing interconnection of cyberspace has introduced complex and evolving challenges to the notion of digital sovereignty, as digital activities increasingly transcend national borders and complicate efforts by states to enforce laws, manage data, and safeguard critical infrastructure. The internet enables cross-border data flows, cyberattacks, and foreign interference, all of which can undermine a state's control over its digital domain. Rapid technological advancements and the ubiquity of cyber incidents now pose significant threats to national sovereignty, often surpassing traditional geopolitical tensions in urgency and impact. In response, states have adopted strategies such as data localization laws and the extraterritorial application of regulations to reassert authority. However, these measures often result in fragmented digital governance, legal conflicts, and diminished global interoperability. To address these risks and prevent the escalation of cyber-related conflicts, international

¹ *Digital 2025 April Global Statshot Report*, <https://datareportal.com/reports/digital-2025-april-global-statshot>, [accessed: 15.08.2025].

cooperation plays a major role in mitigating cyberwarfare and ensuring long-term stability in the digital domain[2].

The friction between digital interconnectivity and national sovereignty has sparked a debate among states over the application of extraterritorial jurisdiction in cyberspace. Traditional notions of territoriality are increasingly ill-suited to the digital environment, where data can be stored virtually anywhere and accessed instantly across borders[3]. To address this challenge, some scholars propose a contextual “weighting test” to guide the exercise of extraterritorial enforcement jurisdiction, balancing all relevant state interests and connections on a case-by-case basis. This approach offers greater flexibility compared to the traditional territorial model. In contrast, other scholars advocate for a pure sovereigntist approach[4], which considers any non-consensual cyber intrusion a violation of international law, reinforcing a strict interpretation of sovereignty as a binding legal rule. These divergent interpretations reflect deeper normative disagreements over how international law should regulate low-intensity cyber operations, particularly those that fall below the threshold of the use of force. As cyberspace continues to evolve, these conflicting approaches will play a crucial role in shaping the future legal landscape of the digital domain.

The NIS 2 Directive (Directive (EU) 2022/2555) was adopted by the European Union in 2022 to strengthen cybersecurity across critical infrastructure and digital services. Member States were required to transpose it into national law by October 17, 2024. As a major revision of the original 2016 NIS Directive, NIS 2 expands the scope of regulated sectors, enhances risk management and incident reporting obligations, and introduces stricter supervisory and enforcement mechanisms. It applies to a wider range of entities, including those in energy, transport, health, digital infrastructure, and public administration.

This paper aims to examine the role of the NIS 2 Directive in reinforcing EU digital sovereignty, particularly amid growing geopolitical competition in cyberspace. It explores how this regulatory framework enhances the EU’s capacity

² Sabir Ijaz, „Cybersecurity and Sovereignty: The Conflict among States in Governing Cyberspace” *Pakistan Social Sciences Review*, No. 4 (2024): 706–714.

³ Cedric Ryngaert, „Extraterritorial Enforcement Jurisdiction in Cyberspace: Normative Shifts” *German Law Journal*, No. 4 (2023): 537–550.

⁴ Kevin Jon Heller, „In Defense of Pure Sovereignty in Cyberspace”, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3895998, [accessed: 15.08.2025].

to secure its digital ecosystem, assert regulatory authority, and shape international cybersecurity norms.

The central question tackled in this paper is: To what extent is NIS 2 a strategic asset or a potential handicap for the European Union in the context of global cyberspace governance and geopolitical rivalry?

By addressing this question, the paper contributes to the ongoing debate on whether NIS 2 strengthens the EU's digital autonomy and resilience or, conversely, whether its stringent regulatory model risks fragmenting the global digital landscape and straining relations with international partners.

2 | General principles applicable in the European Union regarding digitization and cybersecurity

2.1. Information and communication technologies and their importance

In the digital age, information and communication technologies play a pivotal role in facilitating the complex systems that support our daily activities. These technologies drive the European Union's economy in key sectors and strengthen the functioning of the internal market. Greater digitization and interconnectivity also increase the risks associated with these technologies, making society as a whole more vulnerable to cyber threats. Despite the widespread use of information and communication technologies and a high degree of digitization and connectivity, which are now fundamental features of many entities' activities in the EU, their digital resilience is not yet adequate to meet the threats⁵. Information and communication technologies are used extensively in the economic sphere, as well as in everyday life and the public sphere. Their ubiquity means that we are facing an increasing number of cyber threats that affect not only international and national security, but also the performance of work, the provision of services, and basic life activities. It is therefore necessary to build

⁵ Recital 1 of 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 EU L 2022/333/1). It is important to note the need for the secure use of information and communication technologies, which allows for the uninterrupted provision of electronic services vulnerable to cyberthreats, Christophe Gaïe, Mirosław Karpiuk, Nicola Strizzolo, „Cybersecurity of Public Sector Institutions” *Prawo i Więź*, No. 6 (2024): 359, <https://doi.org/10.36128/PRIW.VI53.1129>.

the digital resilience of individuals, societies, states, and the entire European Union, and then global resilience.

The primary goal of digitalization initiatives should be to safeguard Europe's sovereignty, while upholding fundamental European values such as openness and tolerance. Foreign investments in strategic sectors, the acquisition of assets, technologies, and infrastructure of strategic importance in the European Union, and the supply of equipment of significant importance may also pose a threat to the security of the EU[6]. Openness to new technologies must be balanced with a recognition of their potential to compromise security, impacting not only individual users but also nations and the European Union as a whole. In the contemporary business world, technological tools must adhere to established cybersecurity standards. Users must utilize these tools responsibly, possess the necessary knowledge to operate them effectively, and remain cognizant of the potential risks associated with improper usage.

2.2. Cybersecurity threats in the European Union

In the European Union and globally, the scale of cybersecurity incidents is growing. These incidents include attacks on supply chains aimed at cyber espionage, installing ransomware, or causing disruptions. These pose a serious threat to the functioning of networks and information systems. Given the rapid changes in the threat landscape and the high likelihood of large-scale cybersecurity incidents causing serious disruption or damage to critical infrastructure, the European Union needs to be more prepared to respond to them. Such incidents have the potential to disrupt the delivery of public services. Cyberattacks frequently target local, regional, and national infrastructure and public services, leaving local authorities, with their limited resources, particularly vulnerable. These incidents can also hinder economic activity, including in critical sectors, cause significant financial losses, undermine user confidence, and pose a threat to the European Union's economy and democratic systems. It is important to note that cybersecurity incidents are not predictable. They often emerge and evolve at a rapid pace, are not limited to a specific geographical area, and can occur simultaneously or spread rapidly across multiple countries. Countering such incidents requires close collaboration among the public sec-

⁶ Recital 6 of Commission Recommendation (EU) 2019/534 of 26 March 2019 Cybersecurity of 5G networks (OJ EU L 2019/88/42).

tor, private industry, academia, civil society, and the media⁷. Such cooperation is essential for effectively counteracting threats in cyberspace, particularly in the case of large-scale incidents with potential ramifications across multiple EU Member States. Cooperation in the field of cybersecurity is advantageous for several reasons. It reduces the costs of combating cyber threats, minimizes digital exclusion in individual countries, and has a significant impact on building digital solidarity across the European Union.

The digital sovereignty of the European Union necessitates a particular focus on external threats. According to the EU legislator, cyberattacks that constitute an external threat are those that: 1) have been prepared outside the EU or are carried out from outside the EU; 2) use infrastructure located outside the EU; 3) are carried out by a natural or legal person, entity, or body that is established or operates outside the EU; 4) are carried out with the support, on behalf of, or under the control of a natural or legal person, entity, or body that operates outside the EU. Cyberattacks are activities that involve at least one of the following elements: 1) access to information systems; 2) interference with information systems; 3) interference with data; 4) interception of data. These activities will be considered cyberattacks provided that they are not carried out on the basis of a valid authorization issued by the owner or other entity having rights to the system or data or part thereof, or are not permitted under European Union or Member State law. Cyberattacks that pose a threat to Member States include cyberattacks on information systems related to, among other things: 1) critical infrastructure that is essential for maintaining basic social functions or the health, safety, security, and material or social well-being of the population; 2) services essential for the maintenance of basic social or economic activities, in particular in the energy, transport, banking, financial market infrastructure, health, drinking water supply and distribution, digital infrastructure sectors, as well as in any other sector that is essential for the Member State concerned; 3) essential functions of the state, in particular in the areas of defense,

⁷ Recital 2 of Regulation (EU) 2025/38 of the European Parliament and of the Council of 19 December 2024 laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cyber threats and incidents and amending Regulation (EU) 2021/694 (OJ EU L 2025/38). Cybersecurity aims to protect information and communication technology systems from interference that disrupts their normal functioning. This is important because such systems are widely used by both the private sector and public administrations, Dominik Bierecki, Christophe Gaie, Mirosław Karpiuk, „Artificial Intelligence in e-Administration” *Prawo i Więź*, No. 1 (2025): 386, <https://doi.org/10.36128/PRIW.VI54.1201>.

the management and functioning of institutions, the functioning of economic and civil infrastructure, internal security, and external relations; 4) the storage or processing of classified information; 5) the operation of government crisis response teams. In turn, cyberattacks posing a threat to the European Union include cyberattacks carried out against its institutions, bodies, and organizational units, its delegations in third countries or international organizations, its operations and missions conducted in the area of the Common Security and Defence Policy, and its special representatives^[8]. Cyberattacks can vary in nature, both in terms of their territorial scope of impact, including the spread of their effects, and the target at which they are directed. These challenges can be local or national in nature, or they can pose a threat to the European Union. Measures to combat cyberattacks will be taken in proportion to the scale of the threat, bearing in mind that their effects may be difficult to predict, so it is sometimes worth assuming that they may be more severe.

Cybersecurity is a critical component of the digital transformation of the economy and society. The European Union is committed to making investments that will ensure that citizens, businesses, and public authorities can trust digital tools. Given the cross-border nature of cybersecurity threats and the increase in increasingly complex, frequent, and targeted attacks, the relevant institutions and entities involved in cybersecurity should enhance their capacity to respond to such attacks by leveraging existing resources and better coordinating their efforts. All relevant actors in the European Union must be prepared to respond collaboratively and exchange information on a “need-to-share” rather than a “need-to-know” basis^[9]. For the digital transformation to

⁸ Article 1 of Council Decision (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States (OJ EU L 2019/1291/13).

⁹ Recitals 1 and 3 of Commission Recommendation (EU) 2021/1086 of 23 June 2021 on building a Joint Cyber Unit (OJ EU L 2021/237/1). On cybersecurity, see also: Małgorzata Czuryk, „Cybersecurity and Protection of Critical Infrastructure” *Studia Iuridica Lublinensia*, No. 5 (2023): 43–52, <https://doi.org/10.17951/sil.2023.32.5.43-52>; Tomasz Wojciechowski, „Cyberbezpieczeństwo i dezinformacja we współczesnym świecie: strategie ochrony i zarządzania kryzysowego” *Ius et Securitas*, No. 1 (2024): 87–90; Małgorzata Czuryk, „Restrictions on the Exercising of Human and Civil Rights and Freedoms Due to Cybersecurity Issues” *Studia Iuridica Lublinensia*, No. 3 (2022): 31–43, <https://doi.org/10.17951/sil.2022.31.3.31-43>; Patrycja Krauze-Maślankowska, Dorota Majewicz, „Cybersecurity in the Development of Smart Cities: A Big Data Analysis of Digital Security Management Practices by Local Public Administration in Poland” *Ius et Securitas*, No. 2 (2025): 55–66; Dominik Bierecki, Małgorzata Czuryk, Christophe Gaie, Jean Langlois-

proceed smoothly (including in the EU), the involvement of many entities at various stages of the creation and implementation of digital tools is necessary, which is directly related to building resilience to cyber threats. The development of such resilience is intended to facilitate the widespread adoption of new technologies and to safeguard against cyberattacks that could severely disrupt the operation of the IT systems on which these technologies depend.

The use of networks and information systems among citizens, organizations, and businesses throughout the European Union is highly common. Digitization and connectivity are becoming fundamental features of an increasing number of products and services. With the advent of the Internet of Things, an exceptionally large number of connected digital devices are being installed across the EU. Despite the increasing connectivity of devices to the internet, their design often falls short in addressing critical security and resilience aspects, resulting in inadequate protection against cyber threats. In this context, the limited use of certification leads to insufficient knowledge among individual, institutional, and business users about the cybersecurity properties of IT-based services or products. This undermines trust in digital solutions. IT networks and systems have the potential to support all aspects of human life and stimulate economic growth in the European Union. They are a fundamental element in achieving a digital single market^[10]. However, for the digital single market to function optimally, investment in cybersecurity is essential. This is not only a matter of procuring modern tools that are effective in combating cyberattacks, but also of the digital skills of users of information and communication technologies. It is imperative to incorporate cybersecurity measures at the stage of developing digital products or planning the provision of digital ser-

Berthelot, „Sovereignty by Design: Embedding Fiscal Risk Intelligence in Europe's Defence-Digital Strategy” *Prawo i Więź*, No. 1 (2026): 153–156, <https://doi.org/10.36128/2zzk7566>; Krzysztof Kaczmarek, „Bezpieczeństwo państwa wobec współczesnych zagrożeń” *Prawo i Więź*, No. 5 (2025): 568–569, <https://doi.org/10.36128/PRIW.VI58.1382>; Małgorzata Czuryk, „Jurisdiction of the Voivode in the Field of Crisis Management” *Studia Iuridica Lublinensia*, No. 2 (2025): 94–95, <https://doi.org/10.17951/sil.2025.34.2.87-98>; Pierre-Alexandre Boudy, Metodi Hadji-Janev, Mirosław Karpiuk, „The Military Dimension of Cybersecurity” *Studia Iuridica Lublinensia*, No. 1 (2026): 41–61, <https://doi.org/10.17951/sil.2026.35.1.41-61>.

¹⁰ Recital 2 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 and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (OJ EU L 2019/151/15).

vices. It is essential to maintain appropriate cybersecurity standards, which can be certified through the use of specific products and services.

2.3. Cybersecurity policy in the European Union

The European Union has established specific objectives for its cybersecurity policy. These objectives include: 1) promoting a human-centered, fundamental rights-based, transparent, and open digital environment in which secure digital technologies and services comply with and reinforce the principles, rights, and values of the European Union and are accessible to all throughout its territory; 2) strengthening the collective resilience of Member States and bridging the digital divide by developing basic and advanced digital skills; 3) ensuring the strategic digital sovereignty of the European Union while maintaining openness, in particular through secure and accessible digital infrastructure; 4) ensuring access to digital technologies and data on fair terms; 5) developing a comprehensive and sustainable ecosystem of interoperable digital infrastructure, in which large-scale computing, cloud computing, quantum computing, artificial intelligence, and data management operate in a uniform manner, with a view to promoting their use by businesses in the EU and offering new opportunities for economic growth and new jobs; 6) promoting the EU's digital regulatory environment in order to support the ability of EU businesses to compete in the global market; 7) ensuring that everyone can participate online in democratic life and that public services are also available in a trusted and secure online environment for everyone; 8) ensuring that digital infrastructure and technologies become more sustainable, resilient, and energy-efficient; 9) creating non-discriminatory conditions for users in the course of the digital transformation across the European Union by striving for a balance between private and public investment and the use of EU and national funding; 10) ensuring that all policies and programs relevant to the achievement of digital objectives are taken into account in a coordinated and coherent manner; 11) improving resilience to cyberattacks, contributing to risk awareness and spreading knowledge about cybersecurity procedures^[11]. Achieving these overall objectives requires the involvement of many communities, including non-governmental organizations, as well as significant financial resources. It is also important to raise public awareness not only of the benefits of digital transformation, but

¹¹ Article 3 of Decision (EU) 2022/2481 of the European Parliament and of the Council of 14 December 2022 establishing the Digital Decade Policy Programme 2030 (OJ EU L 2022/323/4).

also of the risks that accompany it. Openness to digital tools cannot be unreflective, but must be accompanied by responsibility for their use, as inappropriate use can also generate risks.

3 | Conceptual framework: digital sovereignty, extraterritoriality and cybersecurity

3.1. Defining digital sovereignty

Digital sovereignty refers to a state's capacity to exercise control and authority over its digital infrastructure, data, and activities in service of all national interests. Unlike classic notions of sovereignty, the digital dimension requires considering not only national borders but also all national interests, including, for example, materials and services deployed abroad by national companies. This necessitates ensuring the sovereignty of data, infrastructures, and regulations.

First, protecting data sovereignty is key, as it aims to regulate and control data generated, stored, and processed anywhere the law may be enforced. This power is necessary for safeguarding national security, economic interests, and the privacy of its citizens. Furthermore, ensuring the nation's sovereignty requires controlling critical digital infrastructure, such as internet exchange points, undersea cables, and telecommunications networks, thereby ensuring infrastructure sovereignty. Finally, defining and enforcing laws and regulations in cyberspace enables the enforcement of cybersecurity standards, data governance frameworks, and intellectual property rights without undue influence from external actors. It is important to underline that, as depicted by Couture and Toupin, the concept of digital sovereignty is interpreted differently around the world^[12].

3.2. The principle of extraterritoriality

Extraterritoriality is the principle by which a state applies its laws and jurisdiction beyond its geographical borders. Historically, this has been relevant in areas like maritime law, antitrust regulations, and criminal jurisdiction^[13].

¹² Stéphane Couture, Sophie Toupin, „What Does the Concept of ‘Sovereignty’ Mean in Digital, Network and Technological Sovereignty?“, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3107272, [accessed: 16.08.2025].

¹³ Menno Kamminga, „Extraterritoriality“, <https://opil.ouplaw.com/display/10.1093/law:epil/9780199231690/law-9780199231690-e1040>, [accessed: 16.08.2025].

However, the rise of cyberspace has significantly complicated the application of extraterritoriality. The internet's borderless nature challenges traditional territorial doctrines, which are defined by national laws and international conventions. This complexity arises because data can be stored, accessed, and managed across multiple countries.

Effectively applying extraterritoriality in the digital realm requires defining the roles and responsibilities of all actors involved in digital products and services, as well as determining which state's laws apply. The process hinges on balancing a state's legitimate interest in protecting its citizens and enforcing its laws with the need to prevent legal conflicts and foster international cooperation in cyberspace.

As highlighted by Palladino, the current landscape is characterized by overlapping laws on digital sovereignty that generate geopolitical conflicts and tensions. This is exemplified by policies such as the European Union's General Data Protection Regulation (GDPR), the United States CLOUD Act, and China's National Intelligence Law, all of which assert control over data, leading to potential conflicts and endangering human rights^[14].

3.3. Cybersecurity norms and international law

The rapid evolution of cyber threats has necessitated the development of international cybersecurity norms and principles to govern state behavior in cyberspace. While a comprehensive, universally binding treaty on cybersecurity remains elusive, significant progress has been made through various initiatives and discussions within international forums. Key international cybersecurity norms include the applicability of existing international law, such as the UN Charter's prohibition on the use of force (Article 2(4)), to state conduct in cyberspace.

The UN Group of Governmental Experts (GGE) and the Open-Ended Working Group (OEWG) on cybersecurity have played crucial roles in affirming these principles and developing a framework of responsible state behavior. The GGE,

¹⁴ Nicola Palladino, „The ambiguity of Digital Sovereignty between territorialization of the cyberspace, extraterritorial claims and digital rights: Analysing data transfer policies in EU, US and China”, https://www.giga-net.org/wp-content/uploads/2023/10/GIGANET-2023-Palladino_The-Ambiguity-of-Digital-Sovereignty.pdf, [accessed: 17.08.2025].

through a series of consensus reports^[15], established a foundational framework that includes the applicability of international law, the development of norms for responsible state behavior, confidence-building measures, and capacity building.

Building upon this, the OEWG, established by General Assembly resolution 73/27 in 2018 and later extended through 2025 by resolution 75/240, provides a more inclusive platform for all UN Member States to discuss and advance these norms. Its work encompasses studying threats, examining international law's application, and emphasizing confidence-building and capacity-building initiatives. The OEWG adopted its final substantive report in March 2021 (A/75/816) and continued its work through annual progress reports, culminating in a final report in July 2025^[16]. These efforts aim to reduce miscalculation, promote stability, and foster a more secure cyberspace. However, a significant challenge remains, as Katagiri highlights, in that international law and norms have largely failed to effectively address the actions of non-state actors due to the state-centric nature of traditional international law, creating a "legal void" that complicates maintaining peace and order in cyberspace^[17].

3.4. Combination of the concepts in a competitive cyberspace

In the context of the current competitive cyberspace, there are multiple interdependencies between digital sovereignty, extraterritoriality and cybersecurity norms.

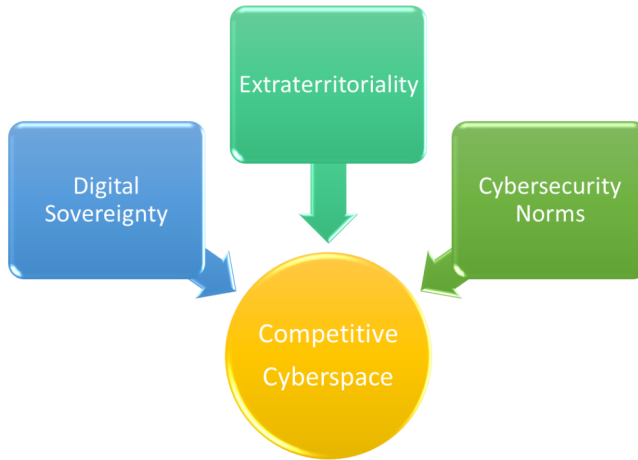
Indeed, states are taking measures to exercise their sovereignty and control over their digital assets, infrastructures, and data, as well as to protect those of their citizens. This is expressed through the identification of what should be controlled and protected in any case. In a geopolitical context of war in Europe and the Middle East, digital sovereignty should also aim to protect the entire supply chain, from the construction of chipsets, graphics processing units, or

¹⁵ *Developments in the field of information and telecommunications in the context of international security*, <https://disarmament.unoda.org/ict-security/>, [accessed: 17.08.2025]; *Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security: note / by the Secretary-General*, <https://digitallibrary.un.org/record/3934214>, [accessed: 17.08.2025].

¹⁶ *UN OEWG concludes, paving way for permanent cybersecurity mechanism*, <https://dig.watch/updates/un-oewg-concludes-paving-way-for-permanent-cybersecurity-mechanism>, [accessed: 20.08.2025].

¹⁷ Nori Katagiri, „Why international law and norms do little in preventing non-state cyber attacks” *Journal of Cybersecurity*, No. 1 (2021): 1–9.

Figure 1. Interdependent relations between digital sovereignty, extraterritoriality and cybersecurity norms



Source: authors.

data servers, to the coding of digital services, as well as ensuring the loyalty of national digital industries, employees, and civil servants.

As sovereignty expands, there is a tendency towards the emergence of extraterritoriality. For instance, the European Union's General Data Protection Regulation (GDPR) applies to any entity processing the data of EU citizens, regardless of the processor's location^[18]. In the meantime, the U.S. CLOUD Act enables American authorities to access data held by U.S.-based companies even if that data resides on servers outside the United States. This practice directly challenges the digital sovereignty of other jurisdictions with conflicting data protection regimes, potentially creating legal uncertainty for multinational technology firms^[19].

The interdependence between sovereignty and extraterritoriality is significantly heightened by the fragmentation of cyberspace. Indeed, the more states attempt to assert control over their digital domains, the more likely they are to infringe upon the sovereignty of others. These tensions may lead to the

¹⁸ Christopher Kuner, *Transborder Data Flows and Data Privacy Law* (Oxford: Oxford University Press, 2013).

¹⁹ Tim Cochrane, „Hiding in the Eye of the Storm Cloud: How CLOUD Act Agreements Expand U.S. Extraterritorial Investigatory Powers” *Duke Journal of Comparative & International Law*, No. 1 (2021): 153–210.

fragmentation of the digital space and the emergence of a “splinternet”^[20] – a patchwork of siloed internets reflecting the boundaries of nation-states. Other possible outcomes include conflict resolution through tribunals or even military operations^[21]. However, the authors argue that a jurisdictional approach, grounded in the development of common legal frameworks, should prevail.

Thus, the negotiation and agreement on international cybersecurity norms should play a central role in peacefully managing cyberspace. To reach this objective, different forums have emerged, such as the United Nations Group of Governmental Experts (UN GGE), which defines norms that establish responsible state behavior in cyberspace^[22]. These include commitments to refrain from targeting critical infrastructure, respecting state sovereignty in cyberspace, and engaging in cooperative mechanisms to mitigate conflict and ensure stability. While not legally binding, these norms serve as soft law instruments aimed at minimizing the destabilizing effects of unilateral extraterritorial assertions and promoting a rules-based approach to cyberspace.

4 | The NIS 2 Directive: requirements and implementation

4.1. Overview of the NIS 2 Directive

The NIS 2 Directive (Directive (EU) 2022/2555) represents a significant evolution of the original 2016 NIS (Network and Information Systems) Directive, which was the European Union’s first piece of EU-wide legislation on cybersecurity. While the original NIS Directive established a foundational baseline for cybersecurity, its implementation proved inconsistent across Member States, highlighting the need for a more comprehensive and harmonized approach to address the growing scale and sophistication of cyber threats. The new directive was published in 2022 to achieve a high common level of cybersecurity across

²⁰ Scott Malcomson, „Splinternet: How Geopolitics and Commerce Are Fragmenting the World Wide Web” *International Journal of Communication*, No. 13 (2019): 642–645.

²¹ Andrew Keane Woods, „Litigating Data Sovereignty”, https://www.yalelawjournal.org/pdf/Woods_i233nhrp.pdf, [accessed: 22.08.2025].

²² Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, <https://dig.watch/wp-content/uploads/2022/08/UN-GGE-Report-2021.pdf>, [accessed: 22.08.2025].

the European Union, with the specific goal of improving the functioning of the internal market. The revised legal framework addresses increased digitization and an evolving threat landscape by adding new sectors and entities to its scope, which in turn improves the resilience and incident response capacities of public and private organizations, competent authorities, and the EU as a whole. Specifically, NIS 2 introduces two categories of sectors: “sectors of high criticality” (Annex I) and “other critical sectors” (Annex II), which are subject to different levels of requirements. The new directive mandates that all Member States must adopt and publish the necessary measures to comply with these enhanced regulations by October 17, 2024[23].

The NIS 2 Directive enhances the EU’s cyber resilience by expanding cybersecurity regulations to more critical sectors. It requires stricter risk management, incident reporting, and enforcement to create a more resilient digital ecosystem. This framework aims to protect vital services and infrastructure from cyberattacks, thereby reinforcing the EU’s digital sovereignty. To ensure compliance, the directive works in tandem with the Cyber Resilience Act (CRA), which focuses on the security of digital products. The paper by Jara et al. uses Libelium’s Libelium One as a practical example to demonstrate how manufacturers can meet these requirements through robust risk management and incident handling[24]. This case study details how the CRA sets standards for IoT devices in critical infrastructures, proving the real-world applicability of these frameworks.

4.2. Key requirements and scope of the NIS 2 Directive

The NIS 2 Directive modernizes its predecessor by broadening its scope, introducing stricter obligations, and creating more robust enforcement mechanisms to create a more secure digital market. It classifies entities based on their criticality[25] into two tiers: essential and important. Essential entities are considered vital to the EU’s economy and society, encompassing sectors like en-

²³ Christophe Gaie, Markus Mueck, „Introduction to the Networks and Information Systems 2 (NIS2) Directive”, [in:] *European Digital Regulations*, eds. Markus Mueck, Christophe Gaie (Cham: Springer, 2025): 161–180.

²⁴ Antonio Jara, Iris Cuevas Martinez, Jaime Sanchez, „CyberSecurity Resilience Act (CRA) in Practice for IoT Devices: Getting Ready for the NIS2”, https://www.researchgate.net/publication/380971234_CyberSecurity_Resilience_Act_CRA_in_practice_for_IoT_devices_Getting_ready_for_the_NIS2, [accessed: 22.08.2025].

²⁵ Jukka Ruohonen, „A Systematic Literature Review on the NIS2 Directive”, <https://arxiv.org/abs/2412.08084>, [accessed: 23.08.2025].

ergy, transport, banking, health, and public administration. These entities are subject to rigorous cybersecurity obligations and proactive supervision. Important entities, a broader category that includes sectors such as postal services, waste management, and manufacturing, must also meet the same core obligations but receive reactive supervision. The classification is primarily based on their involvement in “critical societal or economic activities,” as specified in Article 2 of the directive.

NIS 2 mandates a set of core obligations for all covered entities. First, they must implement comprehensive risk management measures, including cybersecurity policies and incident handling procedures. Second, a structured incident reporting process requires initial alerts to authorities within 24 hours of an incident, followed by a detailed report within 72 hours (Article 23 of the Directive, Reporting obligations). A significant new provision is the focus on supply chain security, which requires entities to assess the risks of their suppliers and service providers. This reinforces the EU’s digital sovereignty by promoting the use of trusted, EU-based suppliers. Finally, the directive places cybersecurity governance squarely on the management body of an entity, with the possibility of personal liability for non-compliance.

Compared to NIS 1, NIS 2’s most significant enhancements are its broader scope, stricter enforcement and fines, and a mandatory focus on supply chain security. The new directive applies to a wider range of sectors and introduces substantial fines for non-compliance, with essential entities facing penalties of up to €10 million or 2% of their global turnover (Article 34, General conditions for imposing administrative fines on essential and important entities). It also enhances cross-border cooperation by establishing networks like EU-CyCLONe to manage large-scale cyber crises at the EU level (Article 16, European cyber crisis liaison organisation network).

The stricter regime does not mean, however, that all covered entities are subject to identical requirements. Article 21(1) of the NIS 2 Directive obliges essential and important entities to take “appropriate and proportionate” technical, operational and organizational measures, and when the proportionality of those measures is assessed, due account must be taken of the degree of the entity’s exposure to risks, its size and the likelihood of occurrence of incidents and their severity, including their societal and economic impact. This is a sector-specific expression of the principle of proportionality laid down in Article 5(4) TEU, which in EU cybersecurity law does not so much narrow the circle of ad-

dressees as adjust the intensity of their obligations to the level of risk^[26]. The same logic underlies the assurance levels of European cybersecurity certification schemes under Article 46(2) of the Cybersecurity Act and the proportionality clause in Article 4 of the Digital Operational Resilience Act (DORA), which ties the ICT risk management obligations of financial entities to their size and overall risk profile and to the nature, scale and complexity of their services, activities and operations^[27]. In NIS 2 itself, proportionality also shapes the scope of the regime and the intensity of supervision: as a rule, the Directive applies only to medium-sized and large enterprises, and important entities are subject only to ex post supervision, whereas essential entities are supervised both ex ante and ex post (Articles 32 and 33).

4.3. Implementation of the NIS 2 Directive

The implementation of the NIS 2 Directive presents significant practical difficulties for both Member States and businesses. The directive's broad scope and stringent requirements introduce a range of challenges, from varying national interpretations to resource allocation and technical compliance issues.

In France, the National Cybersecurity Agency (ANSSI) was highly involved in transposing the directive into national law^[28]. This law was adopted on March 12, 2025. Subsequently, the agency proposed many resources such as the website MonEspaceNIS2 – Directive NIS 2 and the application MonServiceSécurisé. The agency also publishes recommendations to ensure cybersecurity, such as recommendations for using the cloud for entities, available at <https://cyber.gouv.fr/publications/recommandations-pour-lhebergement-des-si-sensibles-dans-le-cloud>.

²⁶ Article 5(4) of the Treaty on European Union (OJ EU C 2012/326/13). See Dominik Bierecki, „The Relevance of the Proportionality Principle under DORA for the Interpretation of the Artificial Intelligence Act in the Context of AI-Based ICT Systems” *Studia Iuridica Lublinensia*, No. 1 (2026): 30–31, <https://doi.org/10.17951/sil.2026.35.1.29-39>.

²⁷ Article 46(2) of Regulation (EU) 2019/881 (Cybersecurity Act) and Article 4 of Regulation (EU) 2022/2554 (DORA), both cited above. On proportionality in DORA, see Dominik Bierecki, „Zasada proporcjonalności w stosowaniu rozporządzenia w sprawie operacyjnej odporności cyfrowej sektora finansowego (Digital Operational Resilience Act – DORA)” *Europejski Przegląd Prawa i Stosunków Międzynarodowych*, No. 3 (2024): 5–13, <https://doi.org/10.52097/eppism.9272>; Bierecki, „The Relevance of the Proportionality Principle...”, 31–32.

²⁸ *Projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité* (PRMD2412608L), <https://www.legifrance.gouv.fr/dossierlegislatif/JORFDOLE000050349138/>, [accessed: 23.08.2025].

Unfortunately, one of the primary difficulties lies in the transposition of the directive into each national law. While NIS 2 is designed to harmonize cybersecurity standards across the EU, it is a minimum harmonization instrument, meaning that Member States are allowed to introduce stricter rules. This can lead to a patchwork of national regulations, creating complexity and legal uncertainty for multinational firms operating across different EU countries. For example, a company operating in multiple Member States might face varying technical requirements or reporting deadlines, complicating its ability to establish a uniform and cost-effective compliance strategy. The lack of a single, definitive interpretation of key terms – particularly regarding what constitutes a “significant incident” or a “serious impact” on services – further exacerbates this issue.

Another major challenge is the substantial burden placed on businesses, especially small and medium-sized enterprises (SMEs) that now fall under the scope of “important entities”. These organizations often lack the financial resources, specialized personnel, and internal expertise needed to meet the directive’s strict risk management and reporting obligations. As a reminder, the EU defines micro and small organizations as those with fewer than 50 employees and less than €10 million in annual revenue; medium-sized organizations as those with 50 to 249 employees and €10 to €50 million in annual revenue; and large organizations as those with 250 or more employees and more than €50 million in annual revenue.

Implementing robust security measures, conducting thorough supply chain risk assessments, and establishing a 24/7 incident response capability can be prohibitively expensive. The new governance requirements, which are heavily compliance-oriented, also introduce a heightened level of risk for business leaders. As a consequence, when decision-makers lack mastery of cybersecurity specifics, they tend to steer their organizations toward compliance rather than true cybersecurity effectiveness – potentially undermining the directive’s intended impact.

This risk shows why proportionality should be treated as an operational tool rather than a declaration. Where the burden on smaller entities becomes excessive, they may respond with a formal, box-ticking approach to compliance instead of directing their limited resources to the areas that generate the greatest risk, which ultimately weakens rather than strengthens their resilience[29]. The

29 Bierecki, „The Relevance of the Proportionality Principle...”, 35.

criteria set out in Article 21(1) of the NIS 2 Directive provide national legislators and competent authorities with an objective benchmark for assessing whether the measures adopted by a given entity are adequate, and for distinguishing genuine shortcomings from the absence of measures that would be disproportionate to its risk profile. Applied consistently, they may also limit divergent supervisory assessments across Member States, which would otherwise compound the fragmentation resulting from minimum harmonization.

Proportionality also matters for the coherence of the growing body of EU cybersecurity law. The obligations of NIS 2 entities coexist with the product requirements of the Cyber Resilience Act, the certification schemes of the Cybersecurity Act, the sector-specific rules for the financial sector laid down in DORA and the cybersecurity requirements for high-risk AI systems under the Artificial Intelligence Act. In some cases, the legislator has resolved the overlap expressly: under Article 4(1) of the NIS 2 Directive, where sector-specific Union legal acts impose requirements at least equivalent in effect, the relevant provisions of the Directive, including those on supervision and enforcement, do not apply, and Article 1(2) of DORA provides that, in relation to financial entities identified as essential or important entities, DORA is to be considered such an act. In other cases, the instruments apply in parallel, each within its own scope, but they rely on the same risk-based method. Article 15(5) of the Artificial Intelligence Act, for instance, requires the technical solutions ensuring the cybersecurity of high-risk AI systems to be appropriate to the relevant circumstances and risks. A systemic interpretation that reads such general clauses in the light of the proportionality criteria of the relevant sectoral regime makes it possible to avoid an accumulation of parallel and partly overlapping obligations without lowering the minimum standards of either instrument^[30].

³⁰ Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (OJ EU L 2024/1689). See Bierecki, „The Relevance of the Proportionality Principle...”, 33–35; Dominik Bierecki, Christophe Gaie, Mirosław Karpiuk, Jean Langlois-Berthelot, „Creating Resilient Artificial Intelligence Systems: A Responsible Approach to Cybersecurity Risks” *Prawo i Więź*, No. 5 (2025): 138–140, <https://doi.org/10.36128/oakf8v90>.

5 | Conclusion

The NIS 2 Directive aims to increase cybersecurity throughout the European Union. It expands the number of entities subject to cybersecurity obligations and requires them to assess the risk of cyberattacks throughout their supply chain. Entities subject to this directive must provide cybersecurity training and audits to their employees. Senior managers are liable for damages caused by failing to comply with mandatory cyber risk management obligations.

Effective cybersecurity crisis management requires cooperation, which may involve exchanging information on cyber threats and cybersecurity incidents, experiences in cybersecurity crisis management, and applicable mechanisms in this area. Cooperation also involves building infrastructure that allows for more effective combating, predicting, and minimizing the effects of cyber threats^[31].

As stated in Recital 105 of the NIS 2 Directive, taking a proactive approach to cyber threats is an essential element of cybersecurity risk management. This approach should allow the relevant authorities to prevent cyber threats from escalating into incidents that could result in significant financial and non-financial damage.

Recital 143 of the NIS 2 Directive clearly states that this legal act does not affect fundamental rights, including the right to privacy and the protection of communications and personal data, the freedom to conduct business, the right to property, the right to an effective remedy and a fair trial, the presumption of innocence, and the right to a defense. However, it introduces significant cybersecurity obligations, which entail considerable financial costs and penalties.

Whether the NIS 2 Directive proves to be a strategic asset or a handicap therefore depends largely on how its proportionality mechanism is applied in practice. If national authorities treat its requirements as a uniform standard to be met in the same way by every entity, the Directive will mainly generate costs, particularly for medium-sized enterprises, and will push them toward formal compliance. If, by contrast, exposure to risk, size and the likelihood and severity of incidents are used to calibrate obligations, the required level of security will reflect actual risk, and NIS 2 can strengthen the Union's resilience and digital sovereignty without disproportionately weakening the competitiveness of

³¹ Małgorzata Czuryk, „Zarządzanie kryzysowe w obszarze cyberbezpieczeństwa” *Ius et Securitas*, No. 1 (2025): 11.

European businesses. Security under NIS 2 should thus be understood not as an absolute benchmark, but as a standard that depends on context and on the likely impact of harm^[32].

It is also important to note sustainable development in the field of cybersecurity. While this aspect is not strongly emphasized in the NIS 2 Directive, the European Union is nevertheless committed to it. To avoid significant harmful effects on the environment and promote a circular economy, digital products and services must be designed, manufactured, used, repaired, recycled, and disposed of in ways that mitigate their negative environmental and societal impacts and prevent premature obsolescence. Everyone should have access to accurate and understandable information about the environmental impact, energy consumption, repairability, and durability of digital products and services so they can make responsible choices.

In the case of strategic sectors covered by the NIS 2 Directive, the energy sector plays an important role. The European energy sector is undergoing a transition towards a low-carbon economy, while ensuring security of supply and maintaining competitiveness. In the context of this energy transition and the associated decentralization of electricity generation from renewable sources, technological progress and digitalization are transforming the European energy network into a “smart grid.” However, these developments bring new risks, as digitalization increasingly exposes the energy system to cyberattacks that could threaten the security of energy supply^[33]. Energy security in a digital Europe is directly linked to the cybersecurity of the energy sector, including mining, electricity, heating, oil, and gas.

Bibliography

Bierecki Dominik, „The Relevance of the Proportionality Principle under DORA for the Interpretation of the Artificial Intelligence Act in the Context of AI-Based ICT Systems” *Studia Iuridica Lublinensia*, No. 1 (2026): 29–39, <https://doi.org/10.17951/sil.2026.35.1.29-39>.

Bierecki Dominik, „Zasada proporcjonalności w stosowaniu rozporządzenia w sprawie operacyjnej odporności cyfrowej sektora finansowego (Digital Operational

³² Bierecki, „The Relevance of the Proportionality Principle...”, 35–37.

³³ Recital 1 of Commission Recommendation (EU) 2019/553 of 3 April 2019 on cybersecurity in the energy sector (OJ EU L 2019/96/50).

- Resilience Act – DORA” *Europejski Przegląd Prawa i Stosunków Międzynarodowych*, No. 3 (2024): 5–13, <https://doi.org/10.52097/epism.9272>.
- Bierecki Dominik, Czuryk Małgorzata, Gaie Christophe, Langlois-Berthelot Jean, „Sovereignty by Design: Embedding Fiscal Risk Intelligence in Europe’s Defence-Digital Strategy” *Prawo i Więź*, No. 1 (2026): 147–164, <https://doi.org/10.36128/2zzk7566>.
- Bierecki Dominik, Gaie Christophe, Karpiuk Mirosław, „Artificial Intelligence in e-Administration” *Prawo i Więź*, No. 1 (2025): 383–407, <https://doi.org/10.36128/PRIW.VI54.1201>.
- Bierecki Dominik, Gaie Christophe, Karpiuk Mirosław, Langlois-Berthelot Jean, „Creating Resilient Artificial Intelligence Systems: A Responsible Approach to Cybersecurity Risks” *Prawo i Więź*, No. 5 (2025): 132–149, <https://doi.org/10.36128/0akf8v90>.
- Boudy Pierre-Alexandre, Hadji-Janev Metodi, Karpiuk Mirosław, „The Military Dimension of Cybersecurity” *Studia Iuridica Lublinensia*, No. 1 (2026): 41–61, <https://doi.org/10.17951/sil.2026.35.1.41-61>.
- Cochrane Tim, „Hiding in the Eye of the Storm Cloud: How CLOUD Act Agreements Expand U.S. Extraterritorial Investigatory Powers” *Duke Journal of Comparative & International Law*, No. 1 (2021): 153–210.
- Couture Stéphane, Toupin Sophie, „What Does the Concept of ‘Sovereignty’ Mean in Digital, Network and Technological Sovereignty?”, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3107272, [accessed: 16.08.2025].
- Czuryk Małgorzata, „Cybersecurity and Protection of Critical Infrastructure” *Studia Iuridica Lublinensia*, No. 5 (2023): 43–52, <https://doi.org/10.17951/sil.2023.32.5.43-52>.
- Czuryk Małgorzata, „Restrictions on the Exercising of Human and Civil Rights and Freedoms Due to Cybersecurity Issues” *Studia Iuridica Lublinensia*, No. 3 (2022): 31–43, <https://doi.org/10.17951/sil.2022.31.3.31-43>.
- Czuryk Małgorzata, „Zarządzanie kryzysowe w obszarze cyberbezpieczeństwa” *Ius et Securitas*, No. 1 (2025): 5–12.
- Czuryk Małgorzata, „Jurisdiction of the Voivode in the Field of Crisis Management” *Studia Iuridica Lublinensia*, No. 2 (2025): 87–98, <https://doi.org/10.17951/sil.2025.34.2.87-98>.
- Gaie Christophe, Karpiuk Mirosław, Strizzolo Nicola, „Cybersecurity of Public Sector Institutions” *Prawo i Więź*, No. 6 (2024): 347–362, <https://doi.org/10.36128/PRIW.VI53.1129>.
- Gaie Christophe, Mueck Markus, „Introduction to the Networks and Information Systems 2 (NIS2) Directive”, [in:] *European Digital Regulations*, eds. Markus Mueck, Christophe Gaie (Cham: Springer, 2025): 161–180.
- Heller Kevin Jon, „In Defense of Pure Sovereignty in Cyberspace”, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3895998, [accessed: 15.08.2025].

- Ijaz Sabir, „Cybersecurity and Sovereignty: The Conflict among States in Governing Cyberspace” *Pakistan Social Sciences Review*, No. 4 (2024): 706–714.
- Jara Antonio, Martinez Iris Cuevas, Sanchez Jaime, „CyberSecurity Resilience Act (CRA) in Practice for IoT Devices: Getting Ready for the NIS2”, https://www.researchgate.net/publication/380971234_CyberSecurity_Resilience_Act_CRA_in_practice_for_IoT_devices_Getting_ready_for_the_NIS2, [accessed: 22.08.2025].
- Kaczmarek Krzysztof, „Bezpieczeństwo państwa wobec współczesnych zagrożeń” *Prawo i Więź*, No. 5 (2025): 567–580, <https://doi.org/10.36128/PRIW.VI58.1382>.
- Kamminga Menno, „Extraterritoriality”, <https://opil.ouplaw.com/display/10.1093/law:epil/9780199231690/law-9780199231690-e1040>, [accessed: 16.08.2025].
- Karpiuk Mirosław, Melchior Claudio, Soler Urszula, „Cybersecurity Management in the Public Service Sector” *Prawo i Więź*, No. 4 (2023): 7–27, <https://doi.org/10.36128/PRIW.VI47.751>.
- Katagiri Nori, „Why international law and norms do little in preventing non-state cyber attacks” *Journal of Cybersecurity*, No. 1 (2021): 1–9.
- Krauze-Maślankowska Patrycja, Majewicz Dorota, „Cybersecurity in the Development of Smart Cities: A Big Data Analysis of Digital Security Management Practices by Local Public Administration in Poland” *Ius et Securitas*, No. 2 (2025): 55–66.
- Kuner Christopher, *Transborder Data Flows and Data Privacy Law* (Oxford: Oxford University Press, 2013).
- Malcomson Scott, „Splinternet: How Geopolitics and Commerce Are Fragmenting the World Wide Web” *International Journal of Communication*, No. 13 (2019): 642–645.
- Palladino Nicola, „The ambiguity of Digital Sovereignty between territorialization of the cyberspace, extraterritorial claims and digital rights: Analysing data transfer policies in EU, US and China”, <https://www.giga-net.org/wp-content/uploads/2023/10/GIGANET-2023-Palladino-The-Ambiguity-of-Digital-Sovereignty.pdf>, [accessed: 17.08.2025].
- Ruohonen Jukka, „A Systematic Literature Review on the NIS2 Directive”, <https://arxiv.org/abs/2412.08084>, [accessed: 23.08.2025].
- Ryngaert Cedric, „Extraterritorial Enforcement Jurisdiction in Cyberspace: Normative Shifts” *German Law Journal*, No. 4 (2023): 537–550.
- Wojciechowski Tomasz, „Cyberbezpieczeństwo i dezinformacja we współczesnym świecie: strategie ochrony i zarządzania kryzysowego” *Ius et Securitas*, No. 1 (2024): 87–90.
- Woods Andrew Keane, „Litigating Data Sovereignty”, https://www.yalelawjournal.org/pdf/Woods_i233nhp.pdf, [accessed: 22.08.2025].

