Instituto Superior Politécnico Gaya
www.ispgaya.pt
https://doi.org/10.58086/625w-1k44

BIBLIOMETRIC ANALYSIS ON CYBERSPACE SECURITY - NIS DIRECTIVES

Cláudia Borgguen[1]

José Morais[2]

Mário Lousã[3]

Abstract

The impact of security in cyberspace has been increasing, motivating companies to reconsider their security strategies. In addition, people from various countries who are aware of this growth are seeking to present studies in various journals that allow them to identify elements that contribute to the consolidation of the concept of security in cyberspace. With this reality in mind, this study, supported by a bibliometric analysis of security in cyberspace based on articles published in the last eight years, aims to analyze the evolution of scientific research, identify the most influential scientific publications on topics related to cyberspace security, and detect research opportunities in the field. The study also discusses the implementation of the legal framework for security in cyberspace and the NIS Directive, aspects that European companies should consider in their cybersecurity strategy. The study's conclusions highlight the multifaceted nature of cybersecurity challenges and the need for a holistic and collaborative approach to strengthening digital resilience, with an emphasis on promoting a culture of awareness encouraged at the organizational and social level by policymakers, industry leaders, and researchers.

Keywords: Security in cyberspace; Cybersecurity; NIS Directive; Legal regime; Bibliometric analysis.

ANÁLISE BIBLIOMÉTRICA SOBRE SEGURANÇA DO CIBERESPAÇO - DIRETIVAS NIS

Resumo

O impacto da segurança no ciberespaço tem vindo a aumentar, motivando as empresas a reconsiderar as suas estratégias de segurança. Além disso, pessoas de vários países que estão atentas a este crescimento procuram apresentar estudos em diversas revistas que lhes permitam identificar elementos que contribuem para a consolidação do conceito de segurança no ciberespaço. Tendo esta realidade em mente, este estudo, apoiado numa análise bibliométrica da segurança no ciberespaço baseada em artigos publicados nos últimos oito anos, tem como objectivo analisar a evolução da investigação científica, identificar as publicações científicas mais influentes sobre temas relacionados com a segurança do ciberespaço, e detectar oportunidades de pesquisa na área. O estudo discute também a implementação do quadro jurídico para a segurança no ciberespaço e a Diretiva NIS, aspectos que as empresas europeias devem considerar na sua estratégia de cibersegurança. As conclusões do estudo destacam a natureza

[1] ISPGAYA /Instituto Superior Politécnico Gaya, Portugal

[2] CEOS.PP; ISPGAYA /Instituto Superior Politécnico Gaya, Portugal

[3] CID ISPGAYA; ISPGAYA /Instituto Superior Politécnico Gaya, Portugal

multifacetada dos desafios de cibersegurança e a necessidade de uma abordagem holística e colaborativa para reforçar a resiliência digital, com ênfase na promoção de uma cultura de sensibilização incentivada a nível organizacional e social por decisores políticos, líderes industriais e investigadores.

Palavras-chave: Segurança no ciberespaço, Cibersegurança, Diretiva NIS, Regime jurídico, Análise bibliométrica.

Introduction

In the last few years, the security of cyberspace has become a fundamental issue for the European Union (EU), demonstrating a strong commitment to promoting a global, open, stable, and secure cyberspace. This commitment is evident in the stance taken by the EU in international security debates related to cyberspace (Salvaggio & González, 2022). One of the main initiatives in this field is the Network and Information Security Directive (NIS), which aims to raise the general level of cybersecurity in the EU (Drivas et al., 2020). The NIS Directive establishes a mandatory reporting regime for operators of essential services and digital service providers, reflecting the EU's determination to strengthen cybersecurity (Franke et al., 2021). Additionally, under the NIS Directive, the European Commission has adopted a comprehensive cybersecurity package to further strengthen the EU's resilience and response to cyberattacks (Maglaras et al., 2020). However, according Cesarec (2020), challenges remain in achieving the highest level of cybersecurity in all EU Member States, indicating gaps in their capabilities.

The legal landscape around cyberspace security in the EU has changed significantly, particularly with the introduction of the NIS Directive and the General Data Protection Regulation (GDPR) (Urquhart & McAuley, 2018). The NIS Directive (Directive (EU) 2016/1148) imposes specific obligations on Member States to improve the cybersecurity posture across the EU (Drivas et al., 2020). In addition, the proposed NIS Directive 2 seeks to modernize the current EU legal framework on cybersecurity and address the limitations of the NIS Directive (Chiara, 2022). Despite these regulatory efforts, there is still a lack of stakeholders in the EU cybersecurity ecosystem, which highlights the need for greater engagement and collaboration (Bederna & Rajnai, 2022).

The increasing exposure to cyber threats due to global interconnectivity requires the adoption of cybersecurity standards and frameworks (Ponsard et al., 2021). The European Union Cybersecurity Act and the NIS Directive play key roles in assisting EU internal market organizations in resisting and recovering from cyber threats (Ferguson, 2022). The NIS Directive is the first EU legal instrument that focuses on incident notification and information sharing as key requirements, highlighting the importance of such information for cyber defense (Ducuing, 2021). Furthermore, the protection of cyberspace has emerged as one of the top security priorities for governments around the world (Carrapico & Farrand, 2016).

This paper is divided into four parts. The first part reviews the literature on cybersecurity, information security, and the NIS Directive. The next part presents the methodology and the research questions, followed by an analysis of the results obtained from the bibliometric analysis. Finally, the final considerations are presented.

1. Literature review

1.1. Cybersecurity

Cybersecurity encompasses the protection of networks and information systems against unauthorized access, use, disclosure, disruption, modification, or destruction of data (Ferguson, 2022). It involves implementing measures to ensure the confidentiality, integrity, and availability of data and services, particularly in critical sectors such as energy, healthcare, and essential services (Biasin & Kamenjašević, 2022; Skias et al., 2021). The NIS and NIS 2 Directives play a crucial role in defining the threshold for reporting cybersecurity incidents and promoting improvements in the cybersecurity of essential services (Schmitz-Berndt, 2023; Wallis & Johnson, 2020).

The dynamic nature of cybersecurity requires taking advantage of information on cyber threats to develop a risk framework that supports decision-making and resilience against them (Riesco & Villagrá, 2019). Additionally, compliance with the NIS Directive requires the development of cybersecurity maturity assessment frameworks to evaluate and improve cybersecurity measures (Drivas et al., 2020). This is exemplified in the case of Greece, where the National Cybersecurity Authority and a cybersecurity framework were created to align with the NIS Directive and ensure the security of critical infrastructure (Maglaras et al., 2020).

1.2. Information security

The term "Information Security" encompasses the protection of data and information systems against unauthorized access, use, disclosure, disruption, modification, or destruction. It involves ensuring the confidentiality, integrity, and availability of information, as well as the systems and processes that store, process, and transmit that information (Schmitz-Berndt & Schiffner, 2021). Information security is crucial for safeguarding sensitive data, such as personal and financial information, intellectual property, and organizational data, from unauthorized access and cyber threats (Wallis & Johnson, 2020). It also involves implementing measures to prevent, detect, and respond to security incidents, including cyberattacks, data breaches, and other security breaches (Skias et al., 2021). In addition, "Information Security" is closely linked to compliance with regulations and standards, such as the NIS Directive, which aims to improve the overall level of cybersecurity in the European Union (Wallis & Johnson, 2020). The NIS Directive gives Operators of Essential Services (OES) responsibility for ensuring the security of networks and information systems, underlining the need for an objective-oriented approach to implementing security and protection standards (Ponsard et al., 2021).

Generally, information security, in the context of the NIS Directive, plays a key role in strengthening the cybersecurity posture of essential services, promoting early detection and adequate mitigation of cybersecurity incidents, and fostering a dynamic risk framework to address emerging cyber threats (Riesco & Villagrá, 2019). Therefore, understanding and defining "Information Security" is essential for organizations to effectively comply with the NIS Directive and contribute to the overall cybersecurity resilience of critical infrastructure and essential services (Bagnato, 2020).

1.3. NIS Directive

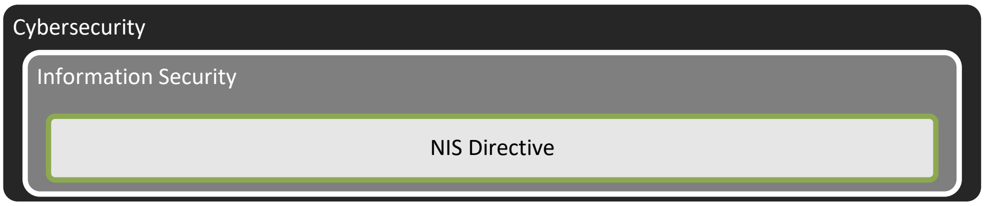
The Network and Information Systems (NIS) Directive is the first EU legal instrument to focus on incident notification and information sharing as key requirements, based on studies showing the importance of such information for cyber defense (Ducuing, 2021). It defines critical infrastructures and operators of essential services, boosting improvements in the cybersecurity of services (Bagnato, 2020; Wallis & Johnson, 2020). It also modernizes the EU's legal framework on cybersecurity and seeks to strengthen the EU's resilience and response to cyberattacks (Ferguson, 2022). The private sector has seen a change in its role in NIS regulation, moving from being the subject of regulation to becoming an active player in policymaking, providing technical expertise for network resilience (Carrapico & Farrand, 2016). In addition, the NIS Directive poses challenges in practice, requiring compliance frameworks and cybersecurity maturity assessments (Biasin & Kamenjašević, 2022).

The NIS Directive has been reformed, leading to the proposal of the NIS 2 Directive, which seeks to modernize the existing EU legal framework on cybersecurity while correcting the shortcomings that prevented the NIS Directive from unlocking its full potential (Chiara, 2022). Furthermore, the NIS Directive has implications for various sectors, including healthcare, as seen in the context of the cybersecurity challenges arising from the AI Act and the NIS 2 Directive proposals for medical devices (Biasin & Kamenjašević, 2022). The literature also emphasizes the importance of dialogue, partnership, and capacity building for network and information security, highlighting the changing role of the private sector from regulatory object to regulatory shaper in the context of the NIS Directive (Carrapico & Farrand, 2016). Overall, the NIS Directive represents a significant step taken by the EU to strengthen the security of networks and information systems, with implications for various sectors and an emphasis on incident reporting, information sharing, and the modernization of cybersecurity legal frameworks.

1.4. Concept relationship

In summary, these three terms are interlinked: the NIS Directive is a legislative measure that establishes standards and requirements for "Information Security" in the EU. In turn, "Information Security" is a subset of the broader field of "Cybersecurity", which encompasses all measures taken to protect digital data and systems. Thus, it can be said that the NIS Directive is part of "Information Security" and that "Information Security" is part of "Cybersecurity" (cf. Figure 1).

Figure 1
Relationship between "Cybersecurity", "Information Security" and the "NIS Directive"



Source: own.

Table 1.
Concepts of "Cybersecurity", "Information Security" and "NIS Directive"

Concept	Description	Authors
Cybersecurity	Cybersecurity involves protecting networks and information systems, particularly in critical sectors, by implementing measures to ensure data confidentiality, integrity, and availability and developing a risk framework and maturity assessment framework in compliance with the NIS Directives.	Drivas et al. (2020); Schmitz-Berndt (2023); Skias et al. (2021)
Information Security	Information Security, in the context of the NIS Directive, involves protecting data and information systems, ensuring their confidentiality, integrity, and availability, safeguarding sensitive data, preventing, detecting, and responding to security incidents, and strengthening the cybersecurity posture of essential services.	Bagnato (2020); Ponsard et al. (2021); Schmitz-Berndt & Schiffner (2021)
NIS Directive	The NIS Directive, the first EU legal instrument focusing on incident notification and information sharing, defines critical infrastructures and operators of essential services, modernizes the EU's cybersecurity legal framework, and has been reformed into the NIS 2 Directive to address its shortcomings and expand its implications to various sectors.	Carrapico & Farrand (2016); Chiara (2022); Ducuing (2021)

2. Methodology

Bibliometric analysis, a quantitative method for evaluating scientific production, has become increasingly popular due to its reliability and efficiency. Zupic and Čater (2014) state that in recent years, there has been an increasing emphasis on advancing theory and practice through bibliometric research (Mukherjee et al., 2022), contributing to a deeper understanding of academic production and its impact. This method involves processing bibliometric data from databases such as Scopus and Web of Science to provide an overview of published scientific articles. According to Ellegaard and Wallin (2015), using statistical tools, researchers can carry out a systematic and transparent review process, allowing bibliographic data to be aggregated to identify the main themes and research trends. However, it is important to note that bibliometric analysis has limitations, such as the consideration of qualitative elements like the impact factor of a journal (Hicks et al., 2015).

The methodology for bibliometric analysis often follows the PRISMA guidelines, which provide a 27-point checklist and a flowchart for preparing systematic reviews and meta-analyses (cf. Figure 2). These guidelines cover several aspects, including the study title, abstract, introduction, methods, results, discussion, and financing, as well as points related to the search strategy, study selection, and data extraction. For Moher (2009), the use of such guidelines guarantees a rigorous and standardized approach to bibliometric analysis, increasing the reliability of the results.

1.1. Research questions

This paper, supported by a bibliometric study, focuses on cyberspace security and the respective implementation of the NIS Directive, and aims to answer the following four research questions:

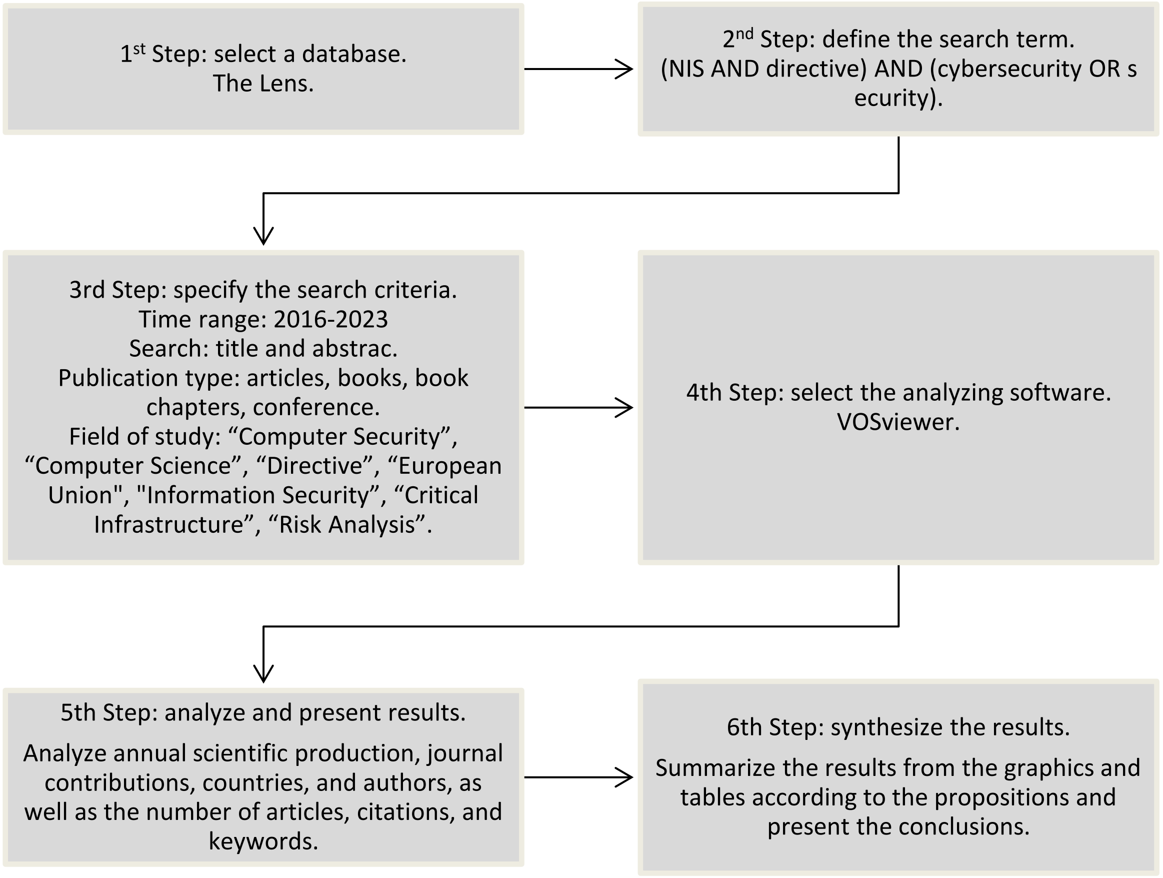
- RQ1: How has the implementation of the legal regime for security in cyberspace and the NIS Directive evolved in academic research over the last eight years?
- RQ2: Which articles stand out most in this topic of study (more citations)?
- RQ3: What are the main focuses of the investigation implementation of the legal regime for security in cyberspace and the NIS Directive?

1.2. PRISMA method

Figure 2 presents the methodology used in the research, based on the PRISMA method. It is observed that six stages were considered to carry out the research: selection of the database; definition of search terms; specification of search criteria; selection of analysis software; analysis and presentation of results; and synthesizing the results.

Figure 2

Methodology



1st Step: select a database.
The Lens.

2nd Step: define the search term.
(NIS AND directive) AND (cybersecurity OR s ecurity).

3rd Step: specify the search criteria.
Time range: 2016-2023
Search: title and abstrac.
Publication type: articles, books, book chapters, conference.
Field of study: “Computer Security”, “Computer Science”, “Directive”, “European Union", "Information Security”, “Critical Infrastructure”, “Risk Analysis”.

4th Step: select the analyzing software.
VOSviewer.

5th Step: analyze and present results.
Analyze annual scientific production, journal contributions, countries, and authors, as well as the number of articles, citations, and keywords.

6th Step: synthesize the results.
Summarize the results from the graphics and tables according to the propositions and present the conclusions.

Source: own.

1.3. Database

The selection of the database for the bibliometric analysis is crucial, and platforms with an extensive collection of patents and academic scientific articles provide valuable data for researchers and students in various fields of science, technology, engineering, and mathematics. Thus, the database chosen was The Lens, a free and open data platform with 144.3 million patents and 252.1 million academic scientific articles and research papers in the fields of science, technology, engineering, and mathematics for researchers and students (The Lens, n.d.).

1.4. Search terms

The terms chosen for the search were "NIS Directive" and "Cybersecurity" from a conjunctive perspective, using the AND operator between the words. So, the query was as follows: (nis AND directive) AND (cybersecurity OR security).

https://doi.org/10.58086/625w-1k44

1.5. Search criteria

The analysis focused on the last eight years, i.e., the search was restricted to publications between 2016 and 2023. Consideration was given to the technical-scientific quality of the type of publication: journal articles, books, book chapters, and conferences. In addition, to obtain specific results within the scope of this study, the following areas of study were selected: "Computer Security", "Computer Science", "Directive", "European Union, Information Security", "Critical Infrastructure", "Risk Analysis".

A total of 340 publications were obtained. A preliminary analysis of the results revealed that some publications did not focus on the research area. So, the search was refined using the fields title, abstract, keywords, and area of study, and 141 publications were obtained. Finally, VOSviewer software version 1.6.20 was used to analyze and visualize the data obtained.

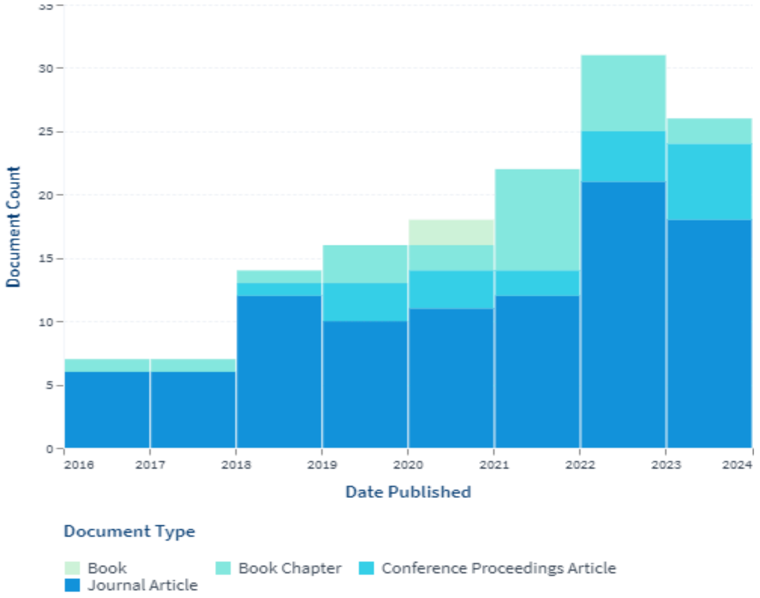
3. Analysis of results

3.1. Descriptive analysis (RQ1 and RQ2)

This study includes 141 documents over a period of eight years, i.e., between 2016 and 2023.

Figure 3 shows the volume of annual scientific production resulting from the research carried out, considering the elements presented in steps 2 and 3 of Figure 2.

Figure 3
Number of publications by type of document



Source: The Lens.

It can therefore be seen that the annual scientific output about the NIS Directive is growing. Considering that 7 documents were published in 2016 and 26 in 2023, the growth is 271%. Attending Table 2, the biggest annual increase was seen in 2022, with 31 publications (two book chapters, six conference proceedings, and 18 articles).

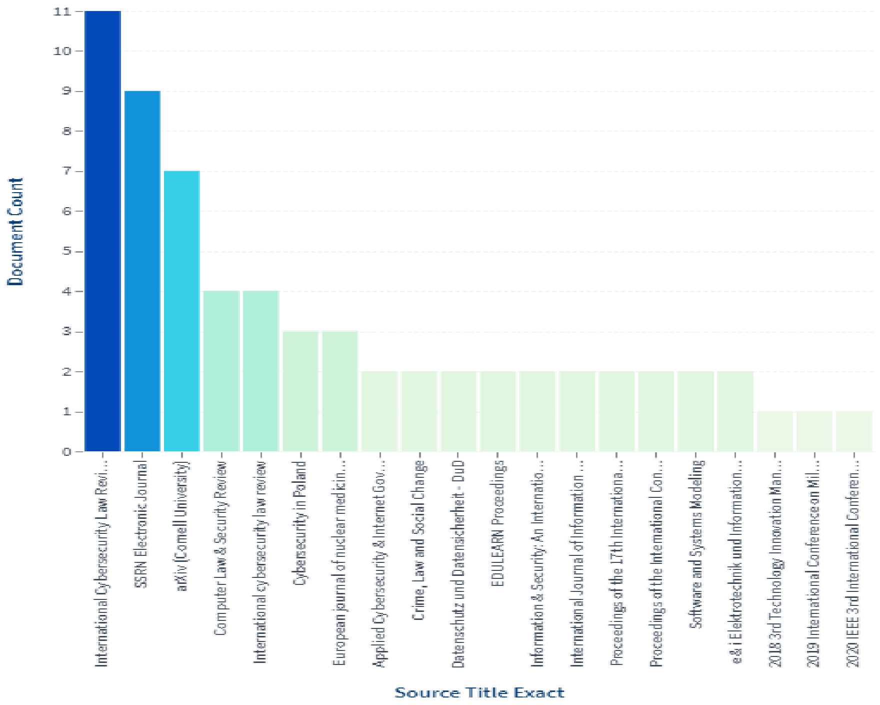
Table 2.
Number of publications by type and year

Year	Books	Book Chapters	Conferences	Articles	Total
2016	-	1	-	6	**7**
2017	-	1	-	6	**7**
2018	-	1	1	12	**14**
2019	-	3	3	10	**16**
2020	2	2	3	11	**18**
2021	-	8	2	12	**22**
2022	-	6	4	21	**31**
2023	-	2	6	18	**26**

Source: The Lens.

The statistics also show that these documents were published in 20 different journals (cf. Figure 4). Table 3 shows the top 5 journals (International Cybersecurity Law Review; SSRN Electronic Journal; arXiv (Cornell University); Computer Law & Security Review; European Journal of Nuclear Medicine and Molecular Imaging) that accounted for 31 publications.

Figure 4
Publications by journal



Source: The Lens.

Table 3

Top 5 journals by number of publications

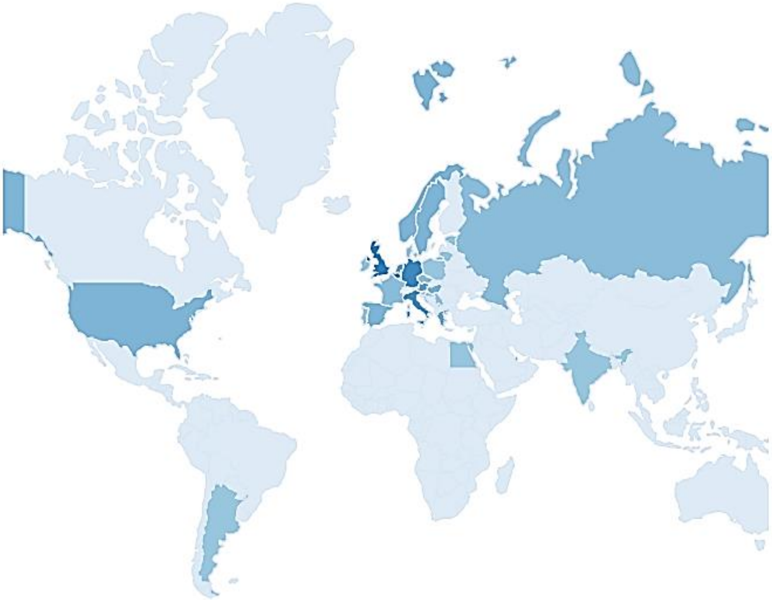
Journal	Field	Number of publications
International Cybersecurity Law Review	Cybersecurity, data security, technology, legislation, and regulation.	15
SSRN Electronic Journal	Social Sciences, Economics, Law, Corporate Governance and Human Sciences.	9
arXiv (Cornell University)	Physics, mathematics, computer science, quantitative biology, quantitative finance, statistics, electrical engineering and systems science, and economics.	7
Computer Law & Security Review	Law, telecommunications regulation, intellectual property, cybercrime, surveillance and security, e-commerce, outsourcing, data protection, e-privacy, EU and public sector IT policy.	4
European Journal of Nuclear Medicine and Molecular Imaging	Physics, dosimetry, radiation biology, radiochemistry, and pharmacy.	3

Source: The Lens.

Figure 5 shows the most active countries in scientific production and research, noting that the countries of the European Union and the United Kingdom have the highest number of publications.

Figure 5

Scientific production by country



Source: The Lens.

Complementing Figure 5, Table 4 illustrates the five countries with the greatest scientific production according to the terms researched. This analysis identifies the countries where there is the greatest concern when investigating the issue of implementing the NIS Directive. It should be noted that the countries with the highest number of publications are on the European continent. This may be because the NIS Directive is, precisely, a European directive.

Table 4

Top 5 countries by number of publications

Country	Number of publications
Belgium	12
United Kingdom	11
Germany	7
Italy	7
Luxembourg	7

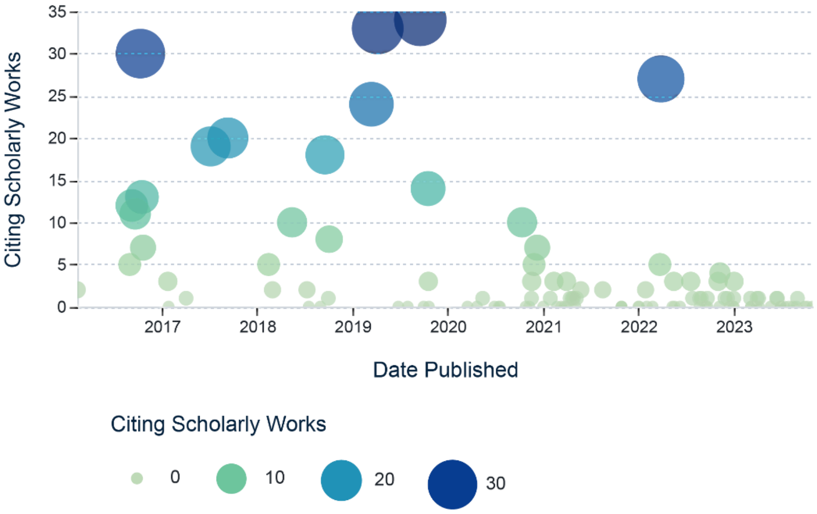
Source: The Lens.

RQ1: Over the past eight years, academic research into the application of the cyberspace security legal regime and the NIS Directive has evolved, resulting in an increasing number of publications covering a wide range of topics (e.g., computer security, scientific computing, business, law, and political science), especially in countries on the European continent.

RQ2: According to Figure 6, there are two articles that stand out, with more than 30 citations. They are: "Dialogue, partnership and empowerment for network and information security: the changing role of the private sector from objects of regulation to regulation shapers", from Carrapico and Farrand (2017), and "Leveraging cyber threat intelligence for a dynamic risk framework" form Riesco and Villagrá (2019).

Figure 6.

Top citations by publication



Source: The Lens.

Table 5 shows the five authors who contributed most to scientific production. Sandra Schmitz-Berndt and George Drivas are the authors with the greatest scientific production, with six publications, followed by Argyro Chatzopoulou, Chris Johnson, and Costas Lambrinoudakis, each with four publications. Again, most authors are based in Europe.

Table 5

Top 5 authors by number of publications

Author	Number of publications
Sandra Schmitz-Berndt	6
George Drivas	6
Argyro Chatzopoulou	4
Chris Johnson	4
Costas Lambrinoudakis	4

Source: The Lens.

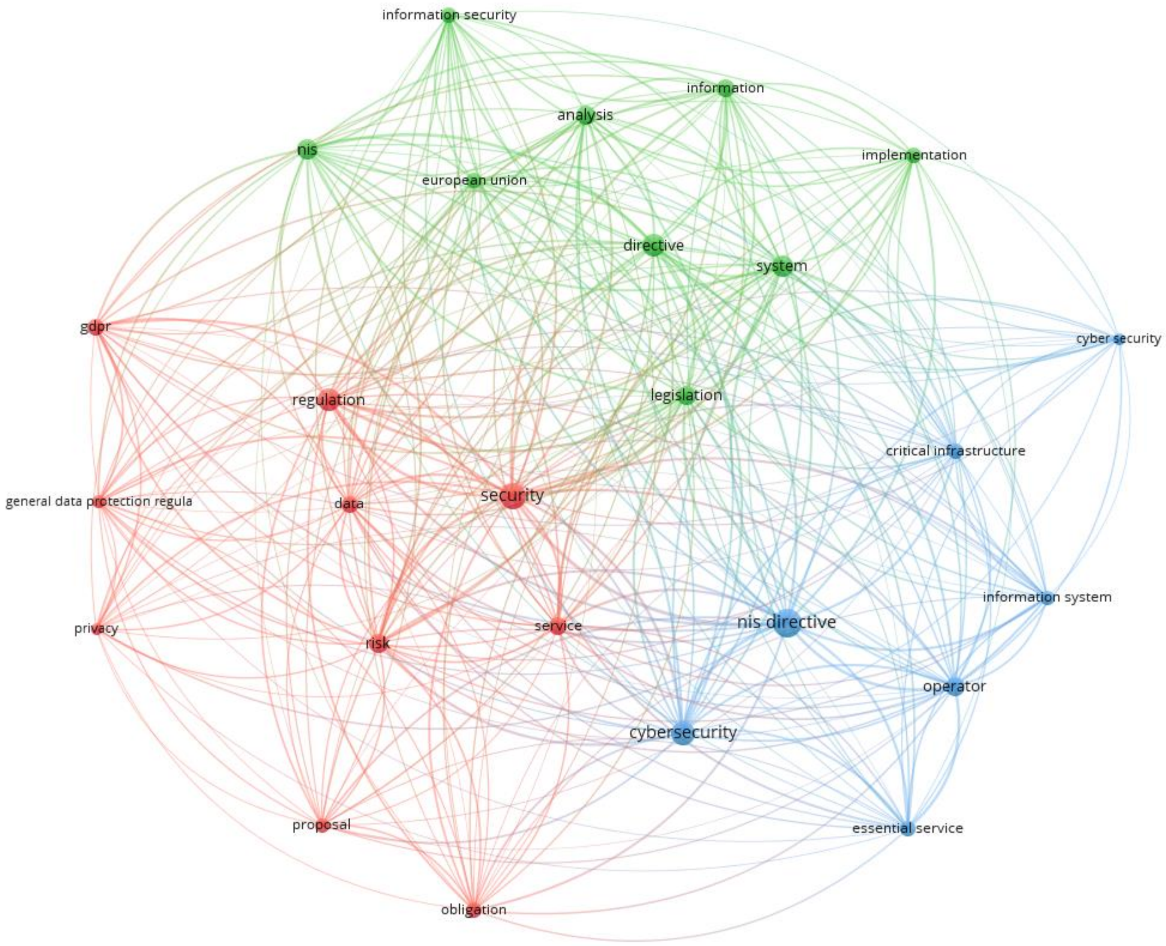
3.2. Keyword analysis (RQ3)

According to Wang and Chai (2018), keyword analysis is an important method for identifying the most relevant publications in a research area, helping to recognize trends and gaps. By examining the most frequent keywords, such as “European Union”, “NIS Directive”, “Regulation” and “Cybersecurity”, it is possible to gain insight into the current focus of the area of investigation. For example, the analysis reveals that the most cited keywords are “NIS Directive” and “Cybersecurity”, indicating a significant emphasis on regulatory frameworks and cybersecurity measures. This suggests a growing concern about the security of information systems and the need for regulatory compliance in the context of cybersecurity.

By examining the most frequent keywords in publications related to these topics, researchers can gain a comprehensive understanding of the evolving landscape of cybersecurity regulation in the European Union. This approach can shed light on the impact of the NIS Directive on cybersecurity practices and the EU's regulatory framework, thus identifying potential areas for further research and development in this critical area.

Using the computer tool VOSviewer, Figure 7 shows the occurrence of the authors' keywords. A minimum of 10 occurrences of a keyword was considered, resulting in a total of 42 keywords distributed across 3 clusters. The largest cluster is the red one, with 10 words in which the keyword "Security" stands out, with 24 occurrences. It is followed by the green cluster with nine words. In this cluster, the keyword "Directive" stands out, with 25 occurrences. Finally, the blue cluster, with seven words, where the keyword "NIS Directive" stands out, with 25 occurrences.

Figure 7
keywords occurrence



Source: VOSviewer.

Table 6 presents the keywords that make up each cluster. In the next section of the paper, each of the clusters is analyzed.

Table 6

Keywords by Cluster

Cluster	Keywords
Red	"data"; "gdpr"; "general data protection regulation"; "obligation"; "privacy"; "proposal"; "regulation"; "risk"; "security"; "service"
Green	"analysis"; "directive"; "european union"; "implementation"; "information"; "information security"; "legislation"; "nis"; "system"
Blue	"critical infrastructure"; "cyber security"; "cybersecurity"; "essential service"; "information system"; "nis directive"; "operator"

Source: VOSviewer.

3.2.1. Red cluster

The keyword sets "data", "gdpr", "general data protection regulation", "obligation", "privacy", "proposal", "regulation", "risk", "security" and "service" cover and interconnect crucial topics in the context of cybersecurity regulation and the NIS Directive. The General Data Protection Regulation (GDPR) has a significant impact on data processing and privacy practices, requiring organizations to comply with strict regulations to ensure the protection of personal data (Torre et al., 2019). GDPR compliance involves several obligations and risks related to data security and privacy, which are essential components of cybersecurity and NIS Directive regulation (Mekovec & Peras, 2020). Remember that, according to Koltay (2016), GDPR also led to a paradigm shift in data governance, emphasizing the importance of data quality, literacy, and management to meet regulatory requirements.

Furthermore, GDPR has triggered the need for organizations to implement robust security measures to protect personal data, thus emphasizing the importance of data security in the context of cybersecurity and NIS Directive regulation (Peloquin et al., 2020). The regulation also requires a comprehensive understanding of GDPR principles and requirements, leading to an assessment of GDPR compliance and its implications in various domains, including, for example, higher education institutions (Penev, 2019). Overall, the set of keywords underscores the multifaceted nature of the GDPR and data-related topics, highlighting their role in shaping cybersecurity practices and regulatory compliance.

3.2.2. Green Cluster

The set of keywords "analysis"; "directive"; "european union"; "implementation"; "information"; "information security"; "legislation"; "nis" and "system" covers interconnected and important topics in the context of cybersecurity and the regulation of the NIS Directive. The NIS Directive, which is the first piece of legislation at the EU level on cybersecurity, aims to achieve a high common level of network and "Information Security" across the European Union. It requires member states to adopt a national strategy for the security of networks and information systems and establishes security and notification requirements for operators of essential services and digital service providers (Pravdiuk, 2023).

Implementing the NIS Directive involves developing and applying information security policies, complying with legal requirements, and adopting information security practices in organizations. This process is essential to ensuring the effectiveness of information security measures and promoting a culture of security awareness and compliance (Park & Chai, 2018). In addition, the NIS Directive highlights the need for functional modeling of information security culture status monitoring systems to assess and improve the level of security in organizations, thus contributing to the overall security of information systems and critical infrastructures (Voitsekhovska et al., 2022).

The NIS Directive also highlights the importance of governance and legislation in relation to information security, seeking to simplify it while at the same time addressing the complexities and challenges associated with ensuring effective governance structures and practices (Fitzgerald & Peltier, 2016).

In summary, the NIS Directive highlights the multifaceted nature of cybersecurity and information security governance, highlighting the interconnected themes of legislation, implementation, analysis, and culture in the context of ensuring the security and resilience of critical infrastructure, information systems, and organizations in the European Union.

3.2.3. Blue Cluster

The set of keywords "critical infrastructure"; "cyber security"; "cybersecurity"; "essential service"; "information system"; "nis directive" and "operator" encompass interconnected and crucial themes in the context of cybersecurity regulation and the NIS Directive. The NIS Directive emphasizes the protection of essential services and information systems, which are integral components of critical infrastructure. It is essential to define critical infrastructures, as they include assets or systems vital to social functions, health, security, and economic well-being, the disruption of which would have a significant impact (Zlateva & Hadjitodorov, 2022). Additionally, the protection of essential services is crucial to preventing attacks and limiting the spread of damage caused by malware, highlighting the importance of cybersecurity in safeguarding critical infrastructure and essential services (Sato et al., 2019).

The integration of information systems into critical infrastructure and essential services is essential to guaranteeing the effective management and protection of these systems. Information systems play a fundamental role in the management and optimization of critical infrastructure resources, thus contributing to the global governance of information systems (Falih et al., 2019). Furthermore, the development of a multidisciplinary cybersecurity workforce is crucial to address the complex challenges associated with protecting critical infrastructure and essential services against cyber threats (Hulatt & Stavrou, 2021). This highlights the importance of a qualified workforce in implementing cybersecurity measures and safeguarding critical infrastructure, information systems, and essential services.

The NIS Directive and cybersecurity practices are also interlinked with the concept of "operator" and the management of information systems in the context of essential services and critical infrastructures (Korablyov & Lutskyy, 2022). The directive highlights the need for a systemic approach to optimizing information technology resources within the framework of information systems governance, aligning with the interconnected themes of "information system" and "essential service" (Falih et al., 2019). The set of keywords therefore underlines the multi-faceted nature of cybersecurity and the regulation of the

NIS Directive, emphasizing its key role in safeguarding essential services and critical infrastructure against cyber threats.

4. Limitations and future research

The results obtained were a consequence of the choices made in stages one to three, as presented in the methodology section, namely the database used and, above all, the words used to support the search. These choices are therefore a limitation of the work carried out.

In future work, it would be relevant to explore the contributions that technology can make to the implementation of cyberspace security regulations. It is important to keep abreast of technological developments. It is therefore suggested that a study be carried out between new technologies, namely Artificial Intelligence and the Internet of Things, and the implementation of NIS 2 in organizations.

5. Conclusion

This bibliometric review paper has provided a comprehensive analysis of the current state of cybersecurity, security in cyberspace, and the application of the NIS and NIS 2 directives. The analysis has highlighted the growing importance of cybersecurity in the digital age as well as the evolving nature of threats in cyberspace.

Firstly, the review highlighted the growing importance of cybersecurity in protecting critical infrastructure, digital services, and personal data. The multiplication of digital technologies and interconnected systems has increased the vulnerability of organizations and individuals to cyber threats. As evidenced by bibliometric analysis, there has been an increase in research output and academic publications focused on cybersecurity, reflecting the growing attention and resources devoted to addressing cyber risks. This underscores the urgency of implementing robust cybersecurity measures to mitigate potential disruptions and protect sensitive information.

Secondly, the review clarified the main components and objectives of the NIS and NIS 2 directives, underlining their role in strengthening the resilience of essential services and digital infrastructures. The directives aim to strengthen cooperation between EU member states, promote risk management practices, and build incident response capabilities to effectively tackle cyber incidents. The review revealed a growing body of literature examining the implications and challenges associated with implementing these directives, highlighting the importance of regulatory frameworks in enhancing cybersecurity preparedness and response.

Additionally, the review highlighted the imperative need to promote a culture of cybersecurity awareness and resilience, both at the organizational and societal levels. Effective cybersecurity measures require not only technological solutions but also a proactive and vigilant mindset on the part of users and stakeholders.

In conclusion, this literature review article has provided valuable insights into the current landscape of cybersecurity, security in cyberspace, and the application of the NIS and NIS 2 directives. The findings highlight the multifaceted nature of cybersecurity challenges and the need for a holistic and collaborative approach to strengthening digital resilience. As the digital ecosystem continues to evolve, it is imperative that policymakers, industry leaders, and researchers remain vigilant and proactive in addressing cyber threats and advancing cybersecurity capabilities.

Bibliographic references

Bagnato, D. (2020). The network information systems directive (EU) 2016/1148: internet service providers and registraties. *Central and Eastern European eDem and eGov Days*, *338*, 111–122. https://doi.org/10.24989/ocg.v.338.9

Bederna, Z., & Rajnai, Z. (2022). Analysis of the cybersecurity ecosystem in the European Union. *International Cybersecurity Law Review*, *3*(1), 35–49. https://doi.org/10.1365/s43439-022-00048-9

Biasin, E., & Kamenjašević, E. (2022). Cybersecurity of medical devices: new challenges arising from the AI Act and NIS 2 Directive proposals. *International Cybersecurity Law Review*, *3*(1), 163–180. https://doi.org/10.1365/s43439-022-00054-x

Carrapico, H., & Farrand, B. (2017). 'Dialogue, partnership and empowerment for network and information security': the changing role of the private sector from objects of regulation to regulation shapers. *Crime, Law, and Social Change*, *67*(3), 245–263. https://doi.org/10.1007/s10611-016-9652-4

Cesarec, I. (2020). Beyond physical threats: Cyber-attacks on critical infrastructure as a challenge of changing security environment – overview of cyber-security legislation and implementation in SEE countries. *Annals of Disaster Risk Sciences*, *3*(1). https://doi.org/10.51381/adrs.v3i1.45

Chiara, P. G. (2022). The Cyber Resilience Act: the EU Commission's proposal for a horizontal regulation on cybersecurity for products with digital elements: An introduction. *International Cybersecurity Law Review*, *3*(2), 255–272. https://doi.org/10.1365/s43439-022-00067-6

Drivas, G., Chatzopoulou, A., Maglaras, L., Lambrinoudakis, C., Cook, A., & Janicke, H. (2020). A NIS directive compliant cybersecurity maturity assessment framework. *2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC)*.

Ducuing, C. (2021). Understanding the rule of prevalence in the NIS directive: C-ITS as a case study. *Computer Law and Security Report*, *40*(105514), 105514. https://doi.org/10.1016/j.clsr.2020.105514

Ellegaard, O., & Wallin, J. A. (2015). The bibliometric analysis of scholarly production: How great is the impact? *Scientometrics*, *105*(3), 1809–1831. https://doi.org/10.1007/s11192-015-1645-z

Falih, N., Jabir, B., & Rahmani, K. (2019). Systemic approach for optimizing information technology resource as a contribution of information system governance. *Indonesian Journal of Electrical Engineering and Computer Science*, *14*(1), 135. https://doi.org/10.11591/ijeecs.v14.i1.pp135-142

Ferguson, D. D. S. (2022). European Cybersecurity Certification Schemes and cybersecurity in the EU internal market. *International Cybersecurity Law Review*, *3*(1), 51–114. https://doi.org/10.1365/s43439-021-00044-5

Fitzgerald, T., & Peltier, T. (2016). *Information security governance simplified: From the boardroom to the keyboard*. CRC Press.

Franke, U., Turell, J., & Johansson, I. (2021). The cost of incidents in essential services—data from Swedish NIS reporting. In *Critical Information Infrastructures Security* (pp. 116–129). Springer International Publishing.

Hicks, D., Wouters, P., Waltman, L., de Rijcke, S., & Rafols, I. (2015). Bibliometrics: The Leiden Manifesto for research metrics. *Nature*, *520*(7548), 429–431. https://doi.org/10.1038/520429a

Hulatt, D., & Stavrou, E. (2021). The development of a multidisciplinary cybersecurity workforce: An investigation. In *Human Aspects of Information Security and Assurance* (pp. 138–147). Springer International Publishing. https://doi.org/10.1007/978-3-030-81111-2_12

Koltay, T. (2016). Data governance, data literacy and the management of data quality. *IFLA Journal*, *42*(4), 303–312. https://doi.org/10.1177/0340035216672238

Korablyov, M., & Lutskyy, S. (2022). System-information models for intelligent information processing. *Innovative Technologies and Scientific Solutions for Industries*, *3(21)*, 26–38. https://doi.org/10.30837/itssi.2022.21.026

Maglaras, L., Drivas, G., Chouliaras, N., Boiten, E., Lambrinoudakis, C., & Ioannidis, S. (2020). Cybersecurity in the Era of Digital Transformation: The case of Greece. *2020 International Conference on Internet of Things and Intelligent Applications (ITIA)*. https://doi.org/10.1109/ITIA50152.2020.9312297

Mekovec, R., & Peras, D. (2020). Implementation of the general data protection regulation: Case of higher education institution. *International Journal of E-Education e-Business e-Management and e-Learning*, *10*(1), 104–113. https://doi.org/10.17706/ijeeee.2020.10.1.104-113

Michelberger, P., & Kemendi, Á. (2020). Data, information and it security - software support for security activities. *Problems of Management in the 21st Century*, *15*(2), 108–124. https://doi.org/10.33225/pmc/20.15.108

Moher, D. (2009). Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement. *Annals of Internal Medicine*, *151*(4), 264. https://doi.org/10.7326/0003-4819-151-4-200908180-00135

Mukherjee, D., Lim, W. M., Kumar, S., & Donthu, N. (2022). Guidelines for advancing theory and practice through bibliometric research. *Journal of Business Research*, *148*, 101–115. https://doi.org/10.1016/j.jbusres.2022.04.042

Park, M., & Chai, S. (2018). Internalization of information security policy and information security practice: A comparison with compliance. *Proceedings of the 51st Hawaii International Conference on System Sciences*.

Peloquin, D., DiMaio, M., Bierer, B., & Barnes, M. (2020). Disruptive and avoidable: GDPR challenges to secondary research uses of data. *European Journal of Human Genetics: EJHG*, *28*(6), 697–705. https://doi.org/10.1038/s41431-020-0596-x

Penev, L. (2019). Data ownership and data publishing. *ARPHA Conference Abstracts*, *2*. https://doi.org/10.3897/aca.2.e39250

Ponsard, C., Grandclaudon, J., & Massonet, P. (2021). A goal-driven approach for the joint deployment of safety and security standards for operators of essential services. *Journal of Software (Malden, MA)*, *33*(9). https://doi.org/10.1002/smr.2338

Pravdiuk, A. (2023). Information security of Ukraine: Information influence and information wars. *European Political and Law Discourse*, *10*(1), 111–121. https://doi.org/10.46340/eppd.2023.10.1.6

Riesco, R., & Villagrá, V. A. (2019). Leveraging cyber threat intelligence for a dynamic risk framework: Automation by using a semantic reasoner and a new combination of standards (STIX^{TM}, SWRL and OWL). *International Journal of Information Security*, *18*(6), 715–739. https://doi.org/10.1007/s10207-019-00433-2

Salvaggio, S. A., & González, N. (2023). The European framework for cybersecurity: strong assets, intricate history. *International Cybersecurity Law Review*, *4*(1), 137–146. https://doi.org/10.1365/s43439-022-00072-9

Sato, Y., Hasegawa, H., & Takakura, H. (2019). Construction of Secure Internal Networks with Communication Classifying System. In *ICISSP* (pp. 552-557). DOI: 10.5220/0007571905520557

Schmitz-Berndt, S. (2023). Defining the reporting threshold for a cybersecurity incident under the NIS Directive and the NIS 2 Directive. *Journal of Cybersecurity*, *9*(1). https://doi.org/10.1093/cybsec/tyad009

Schmitz-Berndt, S., & Schiffner, S. (2021). Don’t tell them now (or at all) – responsible disclosure of security incidents under NIS Directive and GDPR. *International Review of Law Computers & Technology*, *35*(2), 101–115. https://doi.org/10.1080/13600869.2021.1885103

Skias, D., Tsekeridou, S., Zahariadis, T., Voulkidis, A., Velivassaki, T.-H., & Fotiadou, K. (2021). Pan-European cybersecurity incidents information sharing platform to support NIS directive. *Proceedings of the 16th International Conference on Availability, Reliability and Security*. https://doi.org/10.1145/3465481.3470477

The Lens. (n.d.). Explore Global Science and Technology Knowledge. https://www.lens.org/

Torre, D., Soltana, G., Sabetzadeh, M., Briand, L. C., Auffinger, Y., & Goes, P. (2019). Using models to enable compliance checking against the GDPR: An experience report. *2019 ACM/IEEE 22nd International Conference on Model Driven Engineering Languages and Systems (MODELS)*. DOI: 10.1109/MODELS.2019.00-20

Urquhart, L., & McAuley, D. (2018). Avoiding the internet of insecure industrial things. *Computer Law and Security Report*, *34*(3), 450–466. https://doi.org/10.1016/j.clsr.2017.12.004

Voitsekhovska, M. M., Dorosh, M. S., Grechaninov, V. F., & Verenych, O. V. (2022). Functional modeling of the organization’s information security culture state monitoring system development. *Herald of Advanced Information Technology*, *5*(4), 297–308. https://doi.org/10.15276/hait.05.2022.22

Wallis, T., & Johnson, C. (2020). Implementing the NIS Directive, driving cybersecurity improvements for Essential Services. *2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*. DOI: 10.1109/CyberSA49311.2020.9139641

Wang, M., & Chai, L. (2018). Three new bibliometric indicators/approaches derived from keyword analysis. *Scientometrics*, *116*(2), 721–750. https://doi.org/10.1007/s11192-018-2768-9

Zlateva, P., & Hadjitodorov, S. (2022, September). An approach for analysis of critical infrastructure vulnerability to climate hazards. *In IOP Conference Series: Earth and Environmental Science* (Vol. 1094, No. 1, p. 012004). IOP Publishing. DOI 10.1088/1755-1315/1094/1/012004

Zupic, I., & Čater, T. (2015). Bibliometric methods in management and organization. *Organizational Research Methods*, *18*(3), 429–472. https://doi.org/10.1177/109442811456262