Article

Not peer-reviewed version

A Systematic Review of the Term Cyber in European Union Member States' Security Strategies

Petrișor Pătrașcu * , Claudiu-Cosmin Radu , Gabriela-Florina Nicoară

Posted Date: 17 January 2025

doi: 10.20944/preprints202501.1271.v1

Keywords: cyber; national security strategy; EU member states; cyber security; cyber threats; cyber attacks; cyberspace; cyber defense; cyber crime.

doi:10.20944/preprints202501.1271.v1

Article

A Systematic Review of the Term Cyber in European Union Member States' Security Strategies

Petrișor Pătrașcu [1],*, Claudiu-Cosmin Radu [1] and Gabriela-Florina Nicoară [1]

[1] "Carol I" National Defence University, Bucharest, Romania

* Correspondence: patrascupetrisor@yahoo.com

Abstract: In recent years, cybersecurity has gained considerable importance, becoming one of the most significant national security challenges that transcends the physical borders of states. It requires an integrated approach at international level to ensure effective protection of society's information, values and interests in the digital age. The dynamic interaction between technological advancement and the potential for exploitation of vulnerabilities has created a problematic security environment marked by precarious stability. Given the continuing uncertainty related to the magnitude and celerity of socio-technological change, as well as the gradual increase in the use of disruptive cyber tools, managing cyber security remains a highly complex challenge in contemporary political governance. This work presents an analysis of the national security strategies of 21 EU Member States from the perspective of the term cyber, plus other terms derived from it, such as: cyber security, cyber threats, cyber attacks, cyberspace, cyber defense and cyber crime. The application of statistical methodologies clarified the utilization of derivative terms and accentuates their significance in the context of national security. More than that, the results of the analysis are validated through the systematic review of several works in the field.

Keywords: cyber; national security strategy; EU member states; cyber security; cyber threats; cyber attacks; cyberspace; cyber defense; cyber crime

1. Introduction

The evolution of information and communication technology in general, and cyber capabilities in particular, fundamentally have a direct impact on national security [1] (72). Experts in the area believe that cyber security represents a crucial component in achieving socio-economic progress and has emerged as a major component of national policies [2]. Cyber security has become an important issue at both EU and national level. Cyber security is now perceived as part of national security [3]. Most states define cyber security in their national strategic documents and integrate their own concepts of national security and cyber security [1] (p.12). Cybersecurity thus becomes, for most states, an issue to be seen from the perspective of national security and sovereignty. Most states in the world have initiated steps to integrate cyber security into their national security strategies. After numerous failed attempts, often due to poor quality of content or lack of experience, they have succeeded in developing comprehensive national strategies to counter security risks in cyberspace [4] (p. 2). Cybersecurity is considered as the foundation stone of the information society, considering its importance for protecting the availability, integrity and confidentiality of information and digital infra-structure. It therefore requires coherent and detailed strategic planning, adequate legal representation and other related measures [5]. In other news, some authors point out that cyber security has become a highly vicious problem [6]. Given its cross-border nature, it manifests itself at multiple levels, across sectors, across institutions and has a complex impact on all cyber actors, both public and private [7] (p.1). Some authors argue that the lack of effective cyber actions increases vulnerability to cyber attacks [8,9]. In this context, cyber security is becoming increasingly crucial for a nation. To protect its national interests, regional or international, states support the fight against threats in cyberspace by developing cyber security and national security legislation.

This work aims to explore EU Member States' national security strategies and the literature. In practice, the terms found in the text of official documents represent the main key terms that will be the subject of a systematic literature review.

In this context, the proposed objectives are the statistical analysis (Q1) of the term cyber in the national security strategies of the EU member states, the identification (Q2) of the main terms derived from the term *cyber* and their correlation (Q3) with the literature.

To contribute in this way, the present paper aims to answer the following research questions:

Q1. What is the number of occurrences of the term *cyber* in national security strategies? This RQ identifies and analyzes the statistical situation of the term *cyber* in the strategies selected for this study.

Q2. What are the most mentioned terms derived from the main term *cyber*, considering each strategy? This RQ identifies the terms with the highest frequency of occurrence in the analyzed strategies.

Q3. How are terms derived from the main term *cyber* reflected in the literature in the context of national security?

This RQ is based on a systematic literature review.

Figure 1 illustrates the research approach, the paper being organized in five sections. The first section highlights the theoretical considerations underlying the approach. Section 2 presents the research methodology, the results of the analysis of the national strategies, including the presentation of the main key terms. Section 3 presents the systematic literature review by key terms. Section 4 summarizes the research findings. Section 5 provides a brief conclusion of this study, together with identified future research directions.

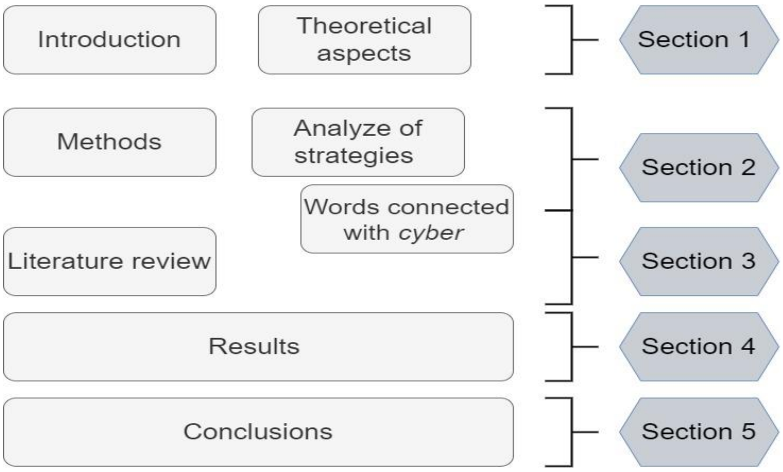


Figure 1. Research methodology outline.

2. Research Methodology

Staging the research approach, the methodology used is schematized in Figure 2. The research methodology is based on a mixed research design consisting of quantitative and qualitative methods. In the first part of the work, content analysis and statistical analysis are used together, and then only qualitative methods are used: structured literature review and content analysis.

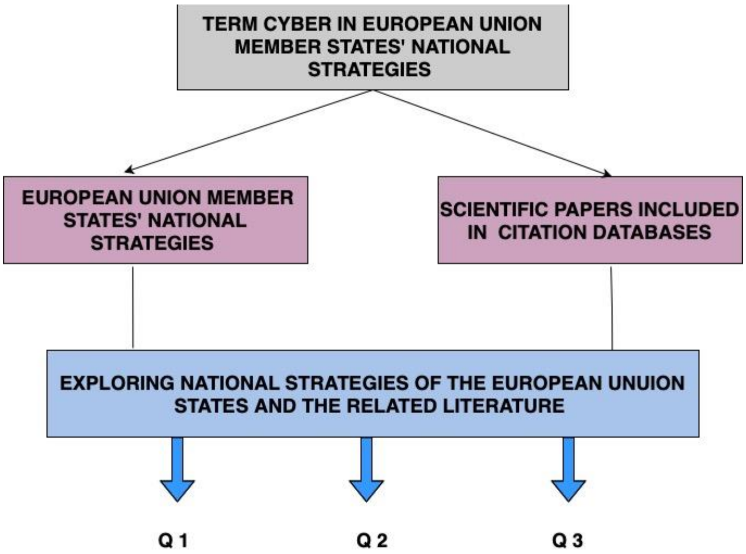

TERM CYBER IN EUROPEAN UNION MEMBER STATES' NATIONAL STRATEGIES
EUROPEAN UNION MEMBER STATES' NATIONAL STRATEGIES
SCIENTIFIC PAPERS INCLUDED IN CITATION DATABASES
EXPLORING NATIONAL STRATEGIES OF THE EUROPEAN UNUION STATES AND THE RELATED LITERATURE
Q 1
Q 2
Q 3

Figure 2. Methodological design.

This study starts with a content analysis that highlights a statistical situation regarding the occurrence of the term *cyber* in the national security strategy documents of the EU Member States. The strategic documents chosen for the study are official acts of the EU Member States, under different titles, such as National Security Strategy (NSS), National Security Concept (NSC), National Defence Strategy (NDS), Foreign and Security Policy Strategy (FSPS), Strategic Concept of National Defence (SCND) and National Strategic Review (NSR). Even if these official documents are found in different forms, justified by a different approach to national security from state to state, they are legal acts that have a common conceptual basis, defining the policies, principles, directions of action and mechanisms necessary to ensure security [10]. Some authors highlight a new generation of national security strategies that have moved from strategies that focus strictly on threats, addressed by military and diplomatic means, to strategies that look at national security in a much broader context, based on the intangibility of the national specificity, of the culture and physical elements within its borders. This is why national security strategies are reviewed at certain periods of time or new ones are developed [11]. In this study, the official documents of the EU Member States, which represent national security strategies or similar documents for national security, are chosen. Details are presented in Table 1.

Table 1. Search criteria.

No	Criteria	Description
1	Database	Google Web Search
2	Keyword of search	The name of the country, followed by "national security strategy" AND "latest version"
3	Date of collection	From July 17 to September 30, 2024
4	Year of publication	In the last 11 years (2013–2024)
5	Type of publication	Official document
6	Integrity	The latest official version
7	Title	Studies focus on the following criteria: national security strategies or similar documents
8	Language	The first option: English; The second option: the official language
9	Full-text analysis	A content analysis that highlights a statistical situation regarding the term "cyber"

The documents analyzed are the latest official versions of the states, openly accessible through Google Web Search, issued by governments, ministries, parliaments and presidential administrations in the period 2013-2024. Table 2 shows the websites where the documents are available. In this context, a total of 21 documents per EU Member State are covered by the study, eliminating from the analysis 6 Member States (Italy, Ireland, Greece, Cyprus, Luxembourg and Malta) due to the non-existence of documents or closed access to them.

Table 2. The national documents and their websites.

Countries	Website
Austria	https://www.bmi.gv.at/502/files/240904_Sichterheitsstrategie_A4_EN_BF.pdf, accessed on 30 September 2024
Belgium	https://www.premier.be/sites/default/files/articles/NVS_Online_EN.pdf, accessed on 17 July 2024
Bulgaria	https://www.me.government.bg/files/useruploads/files/akt.strategiq2020.pdf, accessed on 22 July 2024
Croatia	https://www.soa.hr/files/file/National-Security-Strategy-2017.pdf, accessed on 22 July 2024
Czech Republic	https://mzv.gov.cz/file/5119429/MZV_BS_A4_brochure_WEB_ENG.pdf, accessed on 09 August 2024
Denmark	https://um.dk/en/foreign-policy/foreign-and-security-policy-2023, accessed on 09 August 2024
Estonia	https://www.kaitseministeerium.ee/sites/default/files/eesti_julgeolekupoliitika_alused_eng_22.02.2023.pdf, accessed on 12 August 2024
Finland	https://turvallisuuskomitea.fi/wp-content/uploads/2018/04/YTS_2017_english.pdf, accessed on 16 August 2024
France	https://www.sgdsn.gouv.fr/files/files/rns-uk-20221202.pdf, accessed on 12 August 2024
Germany	https://www.nationalesicherheitsstrategie.de/National-Security-Strategy-EN.pdf, accessed on 19 August 2024
Hungary	https://honvedelem.hu/hirek/government-resolution-1163-2020-21st-april.html, accessed on 2 September 2024
Latvia	https://likumi.lv/ta/en/en/id/345911-on-approval-of-the-national-security-concept, accessed on 2 September 2024
Lithuania	https://kam.lt/wp-content/uploads/2022/03/2017-national-security-strategy.pdf, accessed on 2 September 2024
Netherlands	https://www.government.nl/topics/security-strategy-for-the-kingdom-of-the-netherlands, accessed on 4 September 2024
Poland	https://www.bbn.gov.pl/ftp/dokumenty/National_Security_Strategy_of_the_Republic_of_Poland_2020.pdf, accessed on 4 September 2024
Portugal	https://www.defesa.gov.pt/pt/comunicacao/documentos/Lists/PDEFINTER_DocumentoLookupList/Strategic-Concept-of-National-Defence.pdf, accessed on 4 September 2024
Romania	https://www.presidency.ro/files/userfiles/National_Defence_Strategy_2020_2024.pdf, accessed on 6 September 2024
Slovakia	https://www.mzv.sk/documents/30297/4638226/security-strategy-of-the-slovak-republic.pdf, accessed on 6 September 2024
Slovenia	https://www.gov.si/assets/ministrstva/MO/Dokumenti/R eSNV2.pdf, accessed on 8 September 2024
Spain	https://www.dsn.gob.es/es/documento/estrategia-seguridad-nacional-2021, accessed on 8 September 2024
Sweden	https://www.government.se/globalassets/government/national-security-strategy.pdf, accessed on 8 September 2024

Last but not least, there are other studies that analyze, in a similar way, topics of interest that appear in the national security strategy documents, which further strengthen this scientific approach.

For example, we find papers that focus on the environment and climate change [12], security energy [13] or critical infrastructure protection [14] from a national security perspective.

3. Results

3.1. Statistical Analysis of the Occurrence of the Term Cyber in National Security Strategies

EU Member States have included cyber security aspects in their national security strategies. Threats, vulnerabilities and risks in cyberspace can weaken the security of a state. An analysis of 21 official documents of EU Member States shows their interest in ensuring and strengthening cyber security in the context of national security. Thus, the statistics in Table 3 show that the term cyber is mentioned 602 times in the 21 documents analyzed. The most mentions are found in the strategies of Latvia (76), Germany (62) and France (49). The method of issuing a national security strategy differs from country to country, which is why the timeframe of the strategies analyzed is also much wider (2013-2024). Portugal has a valid strategy issued since 2013, other states update them every a certain period of time, such as Romania (5 years), Estonia and Latvia (4 years). Some states update their national security strategy ahead of the deadline in line with changes in the international security environment and crisis situations. For example, the strategies issued in 2020 (Hungary, Poland, Slovenia, Romania) include elements on the effects of the pandemic on the national health system. The strategies issued after 2022 also emphasize the consequences of Russia's actions in Ukraine (Austria, Belgium, Czech Republic, Estonia, Germany, Netherlands, Latvia, France and Denmark). Also in the context of these last nine strategies (43% of the total number of analyzed documents), the term cyber is mentioned 335 times, which is 55.65%, more than half of the total number of occurrences. Therefore, the results of this section validate RQ1.

Table 3. The statistical situation of mentioning the term cyber in the analyzed national strategies.

Types of document	Countries	No. terms of Cyber	Year	Language
National Security Strategy NSC	Austria	37	2024	English
	Belgium	36	2022	English
	Bulgaria	20	2018	Bulgarian
	Croatia	12	2017	English
	Czech Republic	43	2023	English
	Finland	13	2017	English
	Germany	62	2023	English
	Hungary	36	2020	English
	Lithuania	16	2021	English
	Netherlands	35	2023	English
	Poland	16	2020	English
	Slovakia	24	2021	English
	Slovenia	25	2020	English
	Spain	40	2021	English
	Sweden	13	2017	English
National Defence Strategy NDS	Romania	23	2020	English
National Security Concept NSC	Estonia	5	2023	English
	Latvia	76	2023	English
Strategic Concept of National Defence SCND	Portugal	14	2013	English
National Strategic Review NSR	France	49	2022	English
Foreign and Security Policy Strategy	Denmark	29	2023	

FSPS	English

3.2. *Statistical Analysis of the Most Mentioned Terms Containing the Term Cyber*

This section shows the most mentioned terms in the analyzed documents containing the term *cyber*. Thus, the search returned many terms containing this term (Table 4). The most frequently mentioned terms are cybersecurity (183), cyberspace (120), cyber attacks (99), cyber crimes (39), cyber threats (32) and cyber defense (32). The sum of these terms (505) represents 81% of the total number of 624 mentions presented in the first section. The difference of 19% is found in other terms, such as cyber domain (Czech Republic, Croatia, Finland and Netherlands), cyber incident (Finland, Spain, Lithuania and Netherlands), cyber risk (Bulgaria and France), cyber espionage (Belgium, Czech Republic, Denmark, France, Slovakia, Slovenia and Spain), cyber diplomacy (Austria, Belgium, Denmark, Netherlands and Germany), cyber resilience (Austria, Bulgaria, Czech Republic, France, Germany, Latvia).

Table 4. The most frequently mentioned other terms derived from cyber.

Countries	Cyber attacks	Cyber security	Cyber threats	Cyber space	Cyber defence	Cyber crime
Austria	5	11	0	5	4	5
Belgium	8	12	3	2	1	3
Bulgaria	1	5	0	6	0	2
Croatia	0	0	1	6	0	2
Czech Republic	2	13	5	**14**	1	1
Denmark	11	0	2	3	0	1
Estonia	0	2	0	2	0	1
Finland	0	8	2	0	0	0
France	5	7	1	4	2	1
Germany	**16**	15	0	11	2	1
Hungary	2	9	0	13	**6**	1
Latvia	8	**34**	3	12	3	1
Lithuania	0	11	2	0	2	0
Netherlands	8	11	1	0	0	3
Poland	1	7	2	5	1	0
Portugal	3	2	0	0	2	**6**
Romania	5	3	2	1	1	5
Slovakia	7	6	0	9	1	1
Slovenia	5	7	**7**	2	0	2
Spain	10	11	1	12	0	2
Sweden	2	9	0	13	**6**	1
Total	**99**	**183**	**32**	**120**	**32**	**39**

Figure 3 shows that Latvia has the highest number of mentions, 35 for cyber security. Further, Germany has 16 mentions for cyber attacks, the Czech Republic has 14 mentions for cyberspace, Slovenia has 7 mentions for cyber threats, Portugal has 6 mentions for cyber crimes, and Hungary and Sweden each have 6 mentions for cyber defense. At the same time, there are five countries that have mentioned all six of the terms analyzed in their national security strategies (Belgium, Czech Republic, France, Latvia, Romania).

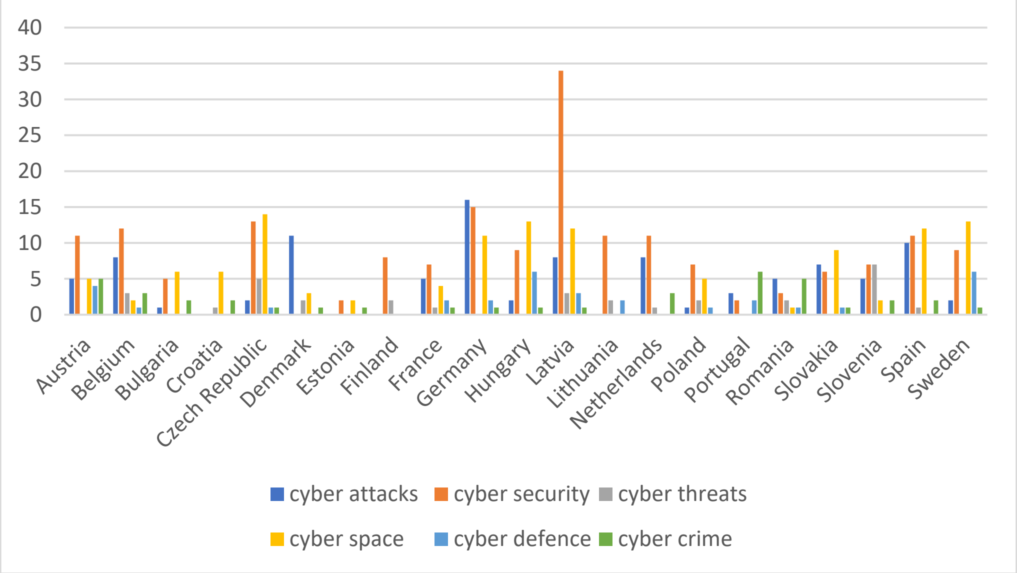


Figure 3. The situation of the terms mentioned by country.

Taking a closer look at the six resulting terms, it can be said that cyberspace is the environment for the other five terms, where cyber attacks, cyber crimes and cyber threats are identified as hostile actions against national security, and are countered by the other two: cyber security and cyber defense. Therefore, it can be said that EU Member States in their national security strategies treat cyberspace in a balanced way from the perspective of threats and attacks, respectively from the perspective of protection, security and even defense of cyberspace.

3.3. Systematic Review of Scientific Literature

The systematic review of the relevant literature in the area focused on identifying the terms derived from the word cyber in the scientific literature and highlighting the integrative whole that defines the issue described by the concept of *cyber*, as it emerges from the content of national documents approved in the countries of the European Union. In this regard, along with the fundamental documents, of strategic level, analyzed in the first stage of the exploratory study, the aim was to identify a specialized content, with a high degree of topicality, focused on the issue under analysis. This step of the research materialized in the following activities:

a. establishing search criteria in relation to *cyber* issues;

b. establishing a preliminary documentation base using the search string;

c. selecting scientific materials considered relevant for content analysis;

d. extracting relevant information, analyzing the extracted information and putting it into context.

a. Establishing search criteria in relation to *cyber* issues

In order to identify content relevant to the described cyber security issue, a number of criteria were established leading to the main directions for querying databases. The choice of the two databases Web of Science and Proquest respectively is justified by the fact that they host globally relevant academic resources. The establishment of the criteria stems from the need to systematize the literature review approach (Table 5). The search was carried out separately for each key term resulting from the analysis of security strategies, while at the same time linking the main term with the "national security" term, as follows:

- ”cyber attack” AND ”national security”;
- ”cyberattack” AND ”national security”;
- ”cybers security” AND ”national security”;
- ”cybersecurity” AND ”national security”;
- ”cyber threats” AND ”national security”;

- ″cyberthreats″ AND ″national security″;
- ″cyber space″ AND ″national security″;
- ″cyberspace″ AND ″national security″;
- ″cyber defence″ AND ″national security″;
- ″cyberdefence″ AND ″national security″;
- ″cyber crime″ AND ″national security″;
- ″cybercrime″ AND ″national security″.

Table 5. The criteria utilized in the establishment of the documentary foundation.

Criteria	Description	Details
Database	Web of Science, Proquest	Data
Keywords	Example: Cyber attack and national security	In the databases, both forms of the phrases specified in the search string must be identified.
Period of time	2013 – September 2024	The selection of this time period is justified by the emergence and development of strategic-level documents from European Union member states addressing the "cyber" domain.
Publication	Dissertations & Theses, Scholarly Journals, Trade Journals	These publications contain relevant articles and papers pertaining to the cybersecurity domain.
Language	English	The security strategies of the Member States of the European Union have English versions.

b. Establishing a preliminary documentation base using the search string

Upon querying the two databases using the search string, 132 results were obtained. These constitute preliminary documentary bases. The process of their establishment was conducted from June to September 2024, and prior to the screening process, duplicate entries were eliminated.

c. Selecting scientific materials considered relevant for content analysis

As a result of the initial search, a total number of 132 papers were retrieved and 9 duplicates across databases were removed before screening. Considering PRISMA guideline [15], the screening process was developed and the papers unrelated to the topic were eliminated, as presented in Figure 4. Taking into consideration the limits of the area of analysis given by EU member states, in the content analysis stage, the articles whose content did not refer to these territorial spaces were not taken into consideration, considering the practices identified in non-EU countries as having low relevance in relation to the objectives set for this research approach. The study selection process was limited to publications written in English, ensuring linguistic consistency across the analyzed materials.

A total of 48 articles were analyzed, taking into account both forms of writing. In the specialized literature we find both forms of writing (bound and unbound) with the same meaning.

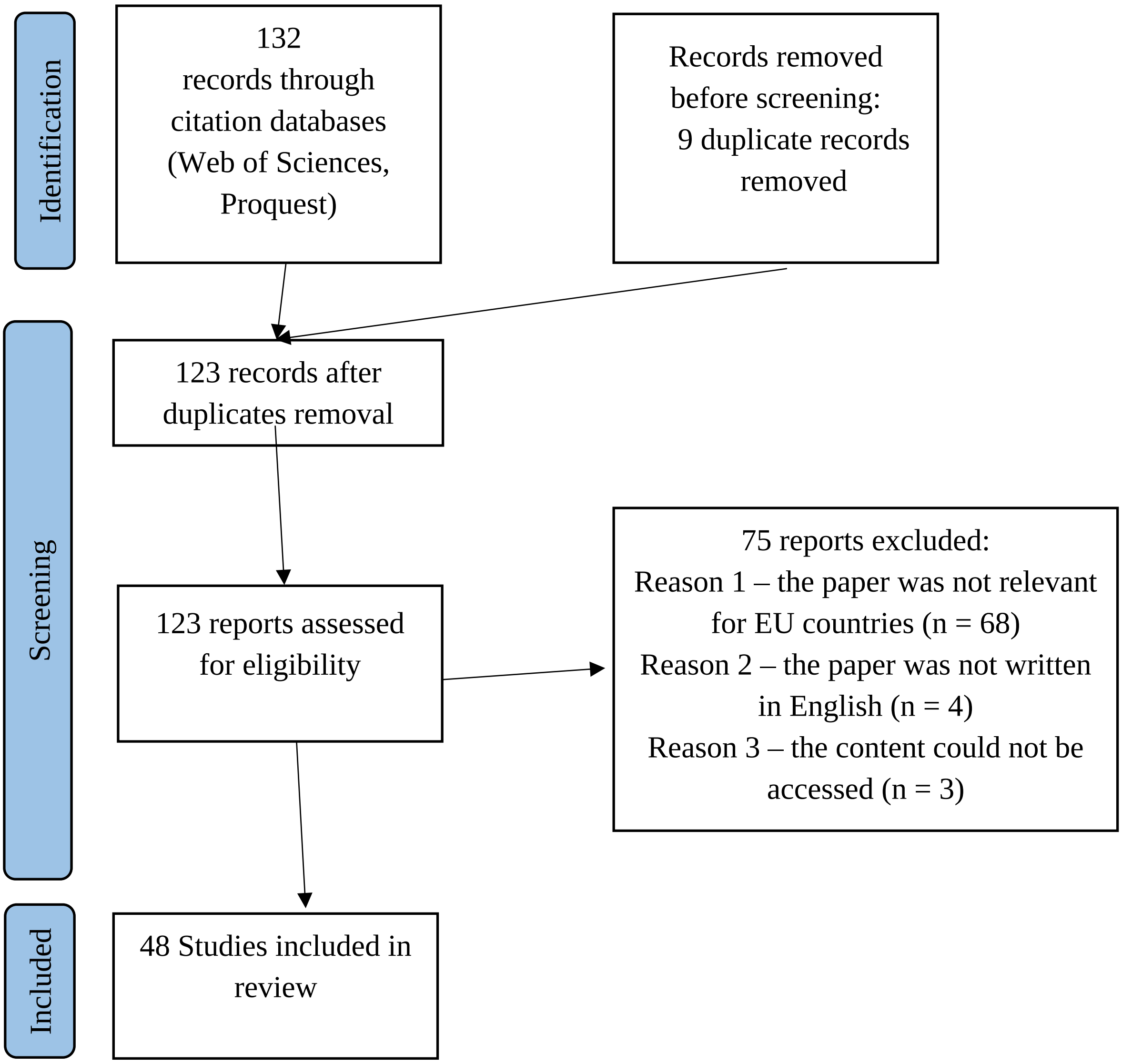


Figure 4. The PRISMA flow diagram.

Even though both variants are correct, we will continue to use the form of the terms corresponding to the largest number of occurrences in the strategies.

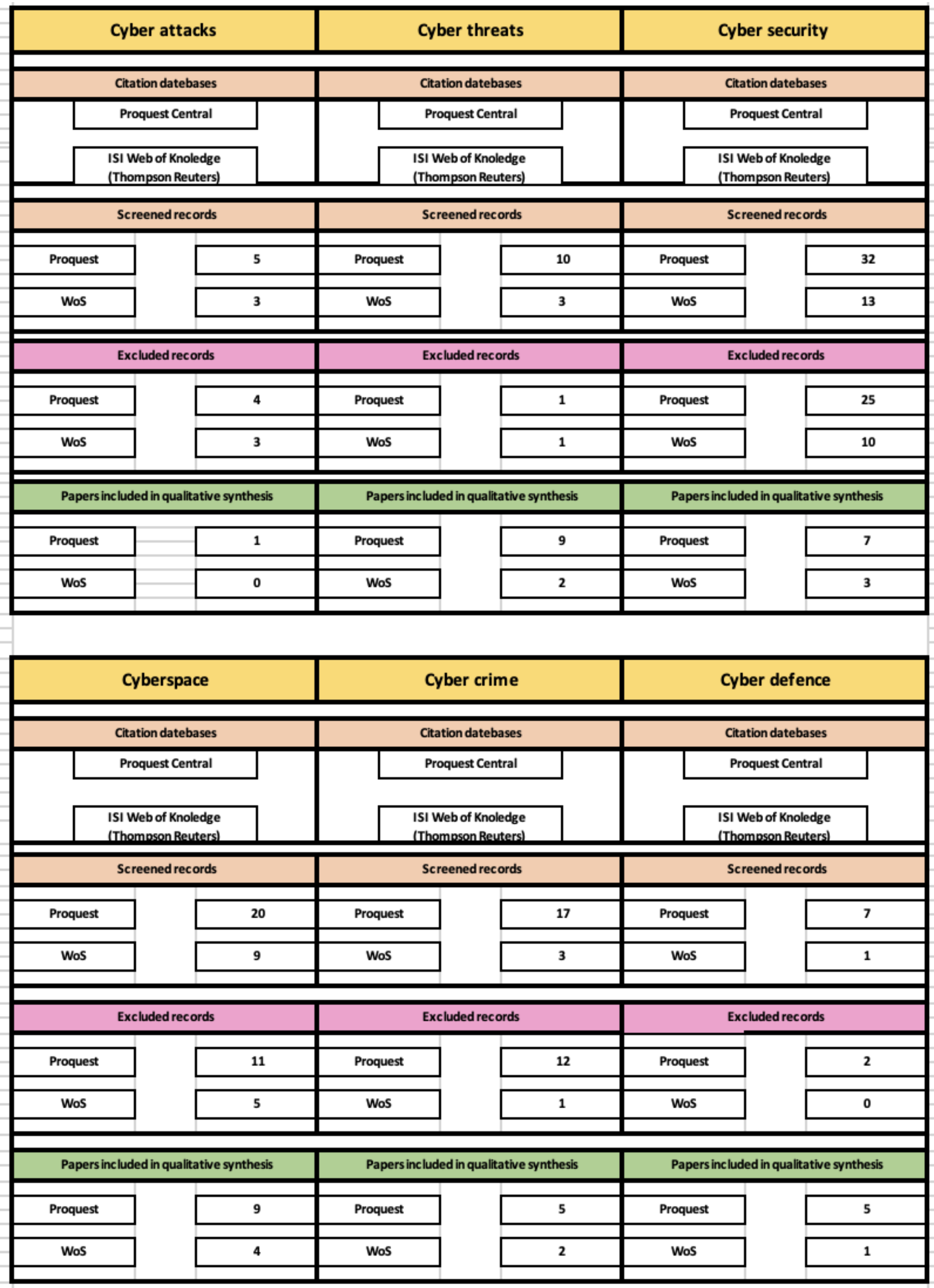
d. Extracting relevant information

Following the specific steps of the literature review, a variable number of articles were selected and analyzed for each term, resulting in the data shown in Table 6.

- *Cyber threats*

Globally, changes in security and defense have led to the emergence and consolidation of a new type of war, namely fourth generation war. Considered to be specific to the information era, there is a direct link between this and the development of cyber threats, a fact supported by Ștefănescu and Papoi, authors who analyze cyber threats in direct correlation with the specific nature of the conflict of the information age [15]. In order to understand the meaning of the term "cyber threats", the two authors explain it in relation to the definition given in the Oxford dictionary, namely "the possibility of a malicious attempt to damage or disrupt a computer network or system" [16].

Table 6. The relevant date of the selection process.



Cyber attacks		Cyber threats		Cyber security	
Citation datebases		Citation datebases		Citation datebases	
Proquest Central		Proquest Central		Proquest Central	
ISI Web of Knoledge (Thompson Reuters)		ISI Web of Knoledge (Thompson Reuters)		ISI Web of Knoledge (Thompson Reuters)	
Screened records		Screened records		Screened records	
Proquest	5	Proquest	10	Proquest	32
WoS	3	WoS	3	WoS	13
Excluded records		Excluded records		Excluded records	
Proquest	4	Proquest	1	Proquest	25
WoS	3	WoS	1	WoS	10
Papers included in qualitative synthesis		Papers included in qualitative synthesis		Papers included in qualitative synthesis	
Proquest	1	Proquest	9	Proquest	7
WoS	0	WoS	2	WoS	3

Cyberspace		Cyber crime		Cyber defence	
Citation datebases		Citation datebases		Citation datebases	
Proquest Central		Proquest Central		Proquest Central	
ISI Web of Knoledge (Thompson Reuters)		ISI Web of Knoledge (Thompson Reuters)		ISI Web of Knoledge (Thompson Reuters)	
Screened records		Screened records		Screened records	
Proquest	20	Proquest	17	Proquest	7
WoS	9	WoS	3	WoS	1
Excluded records		Excluded records		Excluded records	
Proquest	11	Proquest	12	Proquest	2
WoS	5	WoS	1	WoS	0
Papers included in qualitative synthesis		Papers included in qualitative synthesis		Papers included in qualitative synthesis	
Proquest	9	Proquest	5	Proquest	5
WoS	4	WoS	2	WoS	1

In today's society, the Internet is considered as the main electronic platform operated both by public or private actors and by individuals without concrete roles in a formal organizational environment whose operation has multiple security implications [17]. The evolution of society and the increasing level of technological development support the insufficiency of using a classical approach against cyber threats as a means of protection [18], the latter being mostly correlated with the national and international security environment [19].

Under the umbrella of the term “cyber threat”, the specialized literature addresses issues such as:

- easy development of various destructive capabilities and demonstration of their efficiency in attacking computer networks and systems [20]. This is attributable to the use of ineffectively designed barriers and obstacles to cyberspace penetration.

- opening opportunities to the private market by providing the resources to create, build and develop offensive weapons for cyberspace. In this context, there may be problems related to the loss of control in security matters by the governments of the world's states [21]. The migration of cyber expertise to private organizations provides the market with tools and practices that can become threatening and destructive to national security, regardless of its economic and social level of development.

Associated with cyber threats is the concept of cyber attack. Even if the declared topic of the scientific papers refers to the threat, cyber-attack is seen by some authors as a necessary element in clarifying the issue and, consequently, it is introduced in a common context [20],[15]. The regular presence of the two terms in the same scientific context is also justified by the need to provide an integrative framework for analysis of the actors involved, the reasons why they have resorted to these destabilizing actions and their possible consequences. Often, the issue of attribution of blame or identifying who is responsible for a cyber attack is a challenge for the authorities of the responsible states [17].

Hiring cyber mercenaries has become an option for governments in some countries [17]. Due to their professionalism and in-depth knowledge of state-of-the-art technologies, states are inclined to turn to such specialists in order to reduce resources consumed and limit potential losses.

In some states such as Romania, specific rules have been formulated and public authorities and institutions have been nominated responsible for knowing, preventing and countering cyber threats [18]. Even here, however, there is a need to update the definition of cyber threats by including the human element and to reconsider the state's programmatic documents in relation to the new types of cyber threats [18]. Another example of the existing legislative framework is that of Hodgkinson [21], who, by analyzing the legislation, takes steps to identify existing vagueness or ambiguity in the area of cyber threats.

Changes in cyberspace lead to the need to differentiate and name activities, aspects or actors involved in this framework. In this context, the literature brings to the forefront new constructs associated with cyber threats to the security of states such as cyber-mercenaries actions [17] or quantum computing [22].

In essence, cyber threats are perceived as ambiguous, the main argument being the difficulty in identifying similar experiences, actions, activities in previous military conflicts that could serve as a benchmark for comparison. Thus, analogy is limited and novelty is the predominant character. At the same time, the limitations of laws or regulations in the area of security and defense make it impossible to classify cyber threats as acts of war and the incipient stage in the nomination of types of cyber threats support the difficulty in drawing class demarcations in the use of terminology. However, the security context calls with predilection for specialized studies, not only because of the need for states to assess offensive cyber operations, but also in order to be able to counter potential attacks.

- *Cyber attacks*

The second term that comes under attention is “cyber attack”. In recent years, there have been a number of states that have resorted to cyber attacks in order to achieve national security objectives. The ease with which such actions can interfere in the affairs of other states and create major imbalances has led the nations to consider adopting measures of cyber deterrence, collective cyber security and information sharing [23]. A relevant example of a cyber attack that economically affected countries such as Denmark, Ukraine, the United Kingdom and the United States was the ransomware attack called “Petya”or “NotPetya” on June 27, 2017 [23].

On the other hand, the limited number of scientific articles, which fell within the criteria set in the initial stage of the exploration, leads to a series of assumptions regarding the unit of analysis “cyber attack”. There has been noted a lack of tangible research results within the field of national security in relation to the term "cyber attack" in the countries of the European Union associated with national security. A large number of the articles included in the database, but removed on the grounds that they were not relevant to the European Union area, were disseminated by US authors, the content of which concerned analysis from different areas of the United States. Also, the term is found in the content of the articles analyzed above for the term cyber threats. This denotes the incorporation of the concept "cyber attack" into that of "cyber threat".

- *Cyber security*

The term "cyber security" explored in relation to national security through scientific articles provides a fragmented picture of how cyber security issues are viewed by some EU Member States. Digitalization is understood as an integral part of strategic visions of economic growth, prosperity and political inclusion, inseparable from the open market [24].The relevance of the economic field leads to an interest in analyzing the direct link between the cyber security and the digital economy, as the vulnerabilities to which states are exposed as a result of technological change force a reconsideration of international trade law [25].

Petrov [26] approaches cyber security as a dimension of national security by analyzing transnational cybercrime in relation to the use of modern technologies by foreign governments, organizations or individuals. The field to which cyber security applies includes all international informational and telecommunication technologies, and reporting to it requires measures such as monitoring using a unitary framework, educating the agents involved in the improvement of automated control systems in the national security branch [27]. Cyberspace is a man-made field of informational systems, their networks and interconnections that are established between them, behind their management are well-defined organizations and its accelerated transformation in relation to technological evolution calls for the analysis and development of a broad cyber security strategy [28]. Crossing the formal organizational barriers and extending to the national level, Stilius et al. [29] support the same idea of the need for regulation, but emphasize the effect that the lack of international legislation has as well as the potential role of organizations such as NATO or the EU in ensuring cybersecurity. On the other hand, following the analysis carried out by these authors [29], using strategic level documents from the Member States in the European Union, it was pointed out that the existing differences between the characteristics of the nations must be reflected in the specific national legal framework for cybersecurity [29]. Even if states' approaches to securing cyberspace differ, the generic objective pursued by them is to ensure cyber resilience.

Analyzing the security culture in Austria, Haddad and Binder [24] consider the need to reconstruct the relationship between cyber security and digital society in a context described by a new form of globalization. Cyber security in relation to national and international space is considered to be an active place where digital society is collectively negotiated and created, and responsibilities are shared between state, society and individuals. Going beyond state boundaries considers the need for an internationally accepted and supported collective attitude and the internal framework implies an extension of the international framework.

Having as a research objective to explore national and international security and considering the conditions of cyber warfare, Dolzhenkova et al. [30] plead the need for such actions as: UN control using an innovative technical mechanism, signing new treaties under the UN aegis aimed at the protection of personal data, creating a digital learning environment that goes beyond national borders and is aimed at specialized professional education.

An issue present in multiple studies focusing on cyber security is critical infrastructures [11, 16, 18]. Even if the legislation of the states addresses this area in different ways, its presence in multiple scientific analyses highlights the fact that national and cyber security are dependent on critical infrastructure security.

- *Cyberspace*

The fast development of the Internet and computer technologies in recent decades has revolutionized human interactions with the digital environment. At the end of the 20th century, personal computers became increasingly accessible, and the beginning of the 21st century was marked by a significant increase in connectivity, as computers were integrated into global networks. This transition has transformed computers from administrative tools into essential strategic resources in all domains, from the critical ones to day-to-day ones.

With the expansion of the Internet, numerous digital applications and products have been created and have become indispensable in everyday life. Thus, cyberspace has evolved into a global competitive environment where individuals, organizations and governments use technology to improve their efficiency and productivity. This ongoing competition stimulates innovation and development and has a profound impact on socio-economic growth and governance.

In scientific papers, cyberspace is defined as an area where the processing and exchange of information generated by information and communication technology systems takes place. It is also called the essential area that supports the critical infrastructure of a state, enabling business operations, public services and private life. Moreover, some European states are going further with the definition of cyberspace as corresponding to national cyberspace which would violate national security. For example, Poland has introduced the term “cyberspace” of the Republic of Poland, which refers to cyberspace located both on Polish territory and outside of it, in places where representatives of the republic operate [31]. Furthermore, the authors emphasize the importance of cyber situational awareness at the national level in order to protect critical infrastructure and respond effectively to cyber attacks. A discussion is held on the concept of SEZBC (Cyberspace Security Threats Evaluation System), a cyber threat assessment system for national security management in Poland, which aims to improve national decision-making and response capabilities [31].

From an Intelligence point of view, cyberspace is seen as an essential global environment for gathering and analyzing information, having a direct impact on national security. It is used as an area where intelligence operations are conducted to protect national interests against cyber threats [32].

Essentially, “cyberspace” is like a “global ecosystem” that connects the critical infrastructure of all nations and is becoming increasingly vulnerable to attack due to its complexity and interdependencies. It materializes the idea that cyberspace is no longer just a technological area, but also a social and economic one, directly affecting national security [33].

Practically, for about a decade, some authors have included cyberspace as an essential component of the national critical infrastructure, with its protection and defense becoming top priorities. It is also recognized as an operational area, which means that “cyberspace” is being addressed as a new “area of conflict” and a new “operating environment” that is still evolving and not yet fully defined [34]. Moreover, the authors emphasize that cyberspace encompasses all activities of gathering and distributing information through digital technologies, directly influencing national security. Cyberspace is seen as a territory in which nations, terrorist groups, and non-state actors can engage in a wide range of operations, from surveillance to cyber attacks [34]. The same view is supported by Garibaldi and Deane, who define the concept of “cyberspace” as the fifth dimension of warfare, alongside the other four traditional dimensions (land, air, sea and space). Cyberspace is described as a distinct operational environment where warfare can be waged through non-kinetic means, such as attacks on critical infrastructure and information manipulation [35].

Because of its complexity, cyberspace needs to be regulated in the first place, and most European countries are on their second or third iteration of national strategy on cyberspace security. In terms of national security, solutions to challenges in the cyber environment must also include international collaboration to prevent cyber attacks and develop common standards [34]. Some authors argue that governments have a key role in protecting cyberspace against malicious activities and unforeseen incidents. Cyberspace, being an important part of critical national infrastructure, requires security safeguards, especially in the context of new technologies such as cloud-computing and e-banking, which are vulnerable to cyber attacks. Cyber threats can affect the government, public institutions and the national economy, thus emphasizing the need to develop cybersecurity strategies at both government and private sector levels [31].

Vulnerabilities in cyberspace that can be exploited by hostile states or terrorists to cause massive damage to critical infrastructure are increasingly being highlighted. The need for a holistic approach to cyber security, including both defensive measures and offensive capabilities, as part of the national security strategy is being discussed [33]. More and more specialists consider "cyberspace" as a critical area for national security, where information gathering and protection are becoming top priorities. They emphasize that developing cyber capabilities is essential to protect the nation against cyber attacks and cyber espionage [32]. Even though NATO has recognized "cyberspace" as an operational area, state governments must also recognize cyberspace as a battle ground to ensure national security in the modern era. Moreover, traditional defense strategies must be adapted to include cyber capabilities and to protect against threats that are not limited by geographic borders [35].

- *Cyber crime*

Exploring the capabilities of cyber weapons, their lethal potential and the devastating effects they can have, would help to clarify the differences between them and conventional warfare. Due to the lack of clear distinction, the impact of cyber attacks could rival or even exceed the destruction caused by conventional attacks. At the same time, cyber crime is still in the process of being fully recognized and understood in comparison to conventional crime, which requires continuous adaptation of tactics to combat these crimes to keep pace with the fast evolving information technology and internet infrastructure [36].

"Cyber crime" is defined as a phenomenon that uses complex methods to break into computer systems and steal critical data or commit other illegal activities. Cyber criminals are increasingly using sophisticated methods to compromise national and regional economic and financial security [37]. In other words, cyber crime represents any action against the confidentiality, integrity, availability and misuse of computer systems, networks and computer data. These activities include unauthorized access to computer systems, illegal interception of data and illicit transactions with virtual currencies [38]. The acts of virtual criminals may represent one of the greatest threats that society has encountered to date, a result of the fast evolution of technologies which, although developed to make life easier, have opened up new horizons for committing crimes. Cyber crime includes both conventional crimes, adapted to the digital environment, and new types of crimes such as phishing and smishing [39]. Cyber crime, approached as a dynamic and evolving concept, reflects how new technologies have transformed not only society but also the criminal landscape. As technology has developed, traditional crimes have been adapted to the cyber environment and new forms of crime have emerged, taking advantage of the vulnerabilities created by these advanced technologies. Moreover, cyber crime is thus not limited to data theft or online fraud, but also includes much more complex and dangerous activities such as attacks on critical infrastructure, cyber espionage and cyber warfare [40]. The growth of cyber crime in recent years has led some experts to describe "cyber crime" as a "global phenomenon". It includes a wide range of illegal activities carried out through informational and communication technologies. Moreover, these illicit activities range from online fraud to complex attacks on critical infrastructures and are often motivated by economic or political [41]or even religious interests.

In an ever-evolving world, states risk being vulnerable to cyber attacks that can directly affect national security through the vulnerabilities they create in information systems that manage critical information for state security. Countries are already taking the necessary measures to prevent and protect this information to ensure national integrity and security. The development of cyber security strategies is also becoming an integral part of national defense and security measures [38]. Moreover, education in this area is important to ensure national security, as many cyber crimes are transnational in nature and can directly affect national security [39], while international collaboration is becoming essential in developing common cyber security standards for an effective fight against cyber crime [36].

- *Cyber defense*

As far as common standards in the area of cyber defense and cyber security are concerned, EU initiatives are considered appropriate and useful for countries wishing to improve the links between formal policy and its effective and adaptable implementation. The model promoted by the European Union is recognized as an excellent example of best practice in cyber security management at national level. Some countries, such as France, are seeking to align with the model suggested by ENISA in the area of cyber defense and cyber security by emphasizing the particularities of French policies in this area. Cyber defense is seen as a national priority, exemplified by France's “Cyber Defence Pact”, which includes measures to improve cyber threat awareness and monitoring capabilities. In this document, “cyber defense” is defined as a set of nationally coordinated strategies and actions to protect critical infrastructures and information resources against cyber attacks [42]. The development of France's cyber security and cyber defense strategy has focused on creating a unitary approach to domestic cyber risks and threats by increasing cooperation between government agencies, the business sector and academia, and externally by cooperating with other European Union countries to protect government, commerce and individuals [43].

In Romania, cyber defense involves a series of actions carried out in cyberspace for the protection, monitoring, analysis and detection of attacks, with the aim of countering and providing a rapid response to threats to national critical infrastructures [18]. This approach is essential and needs to be reinforced by measures to ensure that public authorities fulfill their duty to adequately inform citizens about matters of public interest [18]. Furthermore, cyber defense can be described as a coordinated national effort to protect critical infrastructures and to prevent, detect and respond to cyber attacks, including proactive and reactive measures that are integrated into a national strategy, with an emphasis on public-private collaboration, education and awareness [44], as is the example of Austria. Kaponig emphasizes that cyber defense is essential to Austria's national security, as protecting critical infrastructure and sensitive information is vital to state stability and sovereignty and without robust cyber defense, vulnerabilities in cyberspace can be exploited by malicious actors, which could lead to economic and social destabilization of the country [44]. Reinforcing this idea, Dumitru and Iuhas consider cyber defense a key element of national security, emphasizing the importance of integrated measures to prevent and combat cyber threats, considering it a national responsibility that involves the protection not only of critical infrastructures, but also of citizens and companies operating in the digital space [45].

4. Discussion and Conclusions

In today's context of cross-border threats and accelerated digitalization, cyber security is no longer an optional component but a central pillar of national security. In the specialized literature it is highlighted that states recognize that cyber security is essential to protect critical infrastructures, classified data and the proper functioning of supply chains and state institutions. The need for integrated cyber policies tailored to each state's context enables quick responses to emerging challenges. This type of approach promotes the adaptability of states by standardizing security policies and integrating cyber security within the national security system. Thus, cyber security and national security are inseparable and states must treat cyberspace as a fundamental component of their security strategy.

Cyber security can also be seen as an operational dimension of modern warfare. Cyberspace recognized as an operational area is of similar strategic importance to other operational areas (land, air, sea, cosmic), where cyber attacks represent direct actions against national sovereignty and integrity. States must therefore take proactive measures and work with international organizations to ensure effective defence capabilities. In an interconnected world, international collaboration is vital to combat sophisticated cyber attacks and to harmonize cyber security standards, which is essential to ensure strengthened national security.

In each of the 21 national security strategies analyzed, we find the term *cyber*. The large number of mentions shows the importance of cyber security in national security. The majority of EU Member States treat threats to cyberspace from a strategic perspective, going well beyond the operational level of cyber security. Moreover, the statistical analysis carried out has extracted the most frequently mentioned terms derived from the term *cyber*. Following the selection, the six most frequently mentioned terms were confirmed, namely: “cyber security”, “cyber threats”, “cyber attacks”, “cyberspace”, “cyber defense”, “cyber crime”. Reflecting on them, it can be observed that the identified terms cover the threat-security correlation, framed in a strategic confrontational environment.

The terms related to the *cyber* concept and resulting from the analysis of national normative acts in European countries were further analyzed using a structured study of the specialized literature. This led to the identification of the current features of the terms proposed for analysis. Each analyzed article provided content elements that were integrated into the picture of the current state of knowledge of the six terms derived from the word *cyber*.

Out of the 27 EU Member States, 21 were considered. However, the remaining six countries have not yet developed or have not yet made public their national security strategies. Therefore, this limitation does not distort the results of the study. Looking at the specialized literature, the analysis of the main terms derived from *cyber* and correlated with the term "national security" provided a limited character to the research, but justified in view of the set objective.

A further research direction could be to extend the study to analyze the national security strategies of other countries outside the European Union and to identify new terms associated with the word *cyber* or to validate those present in this study.

Another research direction can be materialized by analyzing the terms identified in this paper from the perspective of the cyber security strategies of the European Union countries.

Author Contributions: Conceptualization, P.P., C.-C.R. and G.-F.N.; methodology, P.P., C.-C.R. and G.-F.N.; software, P.P., C.-C.R. and G.-F.N.; validation, P.P., C.-C.R. and G.-F.N.; formal analysis, P.P., C.-C.R. and G.-F.N.; investigation, P.P., C.-C.R. and G.-F.N.; resources, P.P., C.-C.R. and G.-F.N.; data curation, P.P., C.-C.R. and G.-F.N.; writing—original draft preparation, P.P., C.-C.R. and G.-F.N.; writing—review and editing, P.P., C.-C.R. and G.-F.N.; visualization, P.P., C.-C.R. and G.-F.N.; supervision, P.P., C.-C.R. and G.-F.N.; project administration, P.P., C.-C.R. and G.-F.N.; funding acquisition, P.P., C.-C.R. and G.-F.N. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Data are contained within the article.

Acknowledgments: The authors thank the reviewers for their thorough reading and helpful comments.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. A. Klimburg, *National Cyber Security Framework Manual*. în NATO CCDCOE Publication. Tallinn, 2012.
2. H. Çifci, „Comparison of National-Level Cybersecurity and Cyber Power Indices: A Conceptual Framework", 2022.
3. D. Stitilis, I. Rotomskis, M. Laurinaitis, S. Nadvynychnyy, și N. Khorunzhak, „National cyber security strategies: management, unification and assessment", *Indep. J. Manag. Prod.*, vol. 11, nr. 9, pp. 2341–2354, nov. 2020, doi: 10.14807/ijmp.v11i9.1431.
4. K. Chałubińska-Jentkiewicz, F. Radoniewicz, și T. Zieliński, *Cybersecurity in Poland Legal Aspects*. în Warsaw. Springer, 2022.
5. D. Štitilis, P. Pakutinskas, M. Laurinaitis, și I. Malinauskaitė-van de Castel, „A Model for the National Cyber Security Strategy. The Lithuanian Case", *J. Secur. Sustain. Issues*, vol. 6, nr. 3, pp. 357–372, 2017, doi: 10.9770/jssi.2017.6.3(3).
6. M. Carr și F. Lesniewska, „Internet of Things, cybersecurity and governing wicked problems: learning from climate change governance", *Int. Relat.*, vol. 34, nr. 3, pp. 391–412, sep. 2020, doi: 10.1177/0047117820948247.
7. M. D. Cavelty și A. Wenger, *Cyber Security Politics Socio-Technological Transformations and Political Fragmentation*. Routledge, London, 2022.
8. V. Bolbot, G. Theotokatos, E. Boulougouris, și D. Vassalos, „A novel cyber-risk assessment method for ship systems", *Saf. Sci.*, vol. 131, p. 104908, nov. 2020, doi: 10.1016/j.ssci.2020.104908.

9. Ö. Aslan, S. S. Aktuğ, M. Ozkan-Okay, A. A. Yilmaz, și E. Akin, „A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions", *Electronics*, vol. 12, nr. 6, 2023, doi: 10.3390/electronics12061333.
10. D. A. Lipinsky, V. V. Bolgova, A. A. Musatkina, A. V. Azarkhin, și A. P. Korobova, „General Social Values in National Security Strategies of the Russian Federation and Germany", *AD Alta J. Interdiscip. Res.*, 2019.
11. S. L. Caudle și S. de Spiegeleire, „A New Generation of National Security Strategies: Early Findings from the Netherlands and the United Kingdom", vol. 7, nr. 1, 2010, doi: 10.2202/1547-7355.1679.
12. A. Vogler, „Barking up the tree wrongly? How national security strategies frame climate and other environmental change as security issues", *Polit. Geogr.*, vol. 105, p. 102893, aug. 2023, doi: 10.1016/j.polgeo.2023.102893.
13. D. Mara, S. Nate, A. Stavytskyy, și G. Kharlamova, „The Place of Energy Security in the National Security Framework: An Assessment Approach", *Energies*, vol. 15, nr. 2, 2022, doi: 10.3390/en15020658.
14. P. Pătrașcu, „National Security Strategies and Critical Infrastructure: An Analysis of the European Union Member States", *Romanian Mil. Think.*, vol. 2022, pp. 10–29, sep. 2022, doi: 10.55535/RMT.2022.3.01.
15. D. Stefanescu și A. Papoi, „NEW threats to the national security of states ⇓ Cyber threat", *Sci. J. Silesian Univ. Technol. Ser. Transp.*, vol. 107, pp. 177–182, iun. 2020, doi: 10.20858/sjsutst.2020.107.13.
16. „Oxford Dictionary". [Online]. Disponibil la: https://en.oxforddictionaries.com/definition/cyberthreat
17. Jose de Arimateia da Cruz, „Cyber Mercenaries: A New Threat to National Security", *Int. Soc. Sci. Rev.*, vol. 96, 2020.
18. S. A. Manea, „Implications of the evolution of cyber threats on the duties of actors in the field of security and national defense", *Int. Sci. Conf. Strateg. XXI Suppl Glob. Secur. Natl. Def.*, pp. 213–217, 2020.
19. A. Dinicu, „Cyber threats to national security. Specific features and actors involved", *Sci. Bull. - Nicolae Balcescu Land Forces Acad.*, vol. 19, nr. 2, pp. 109–113, 2014.
20. G.-D. Bobric, „Study Regarding the Cyber Threats to the National Security", *Sci. Bull.*, vol. 25, pp. 18–25, iun. 2020, doi: 10.2478/bsaft-2020-0003.
21. „Crossing the Line: The Law of War and Cyber Engagement - Crossing the Line: The Law of War and Cyber Engagement - Applying the Existing Body of Law to This New National Security Applying the Existing Body of Law to This New National Security Threat", *Int. Lawyer*, vol. 51 (3), pp. 613–628, 2018.
22. S. Grobman, „Quantum Computing's Cyber-Threat to National Security", *Prism J. Cent. Complex Oper.*, vol. 9, nr. 1, pp. 52–66, 2020.
23. J. Osawa, „The Escalation of State Sponsored Cyberattack and National Cyber Security Affairs: Is Strategic Cyber Deterrence the Key to Solving the Problem?", *ASIA-Pac. Rev.*, vol. 24, nr. 2, pp. 113–131, 2017, doi: 10.1080/13439006.2017.1406703.
24. C. Haddad și C. Binder, „Governing through cybersecurity: national policy strategies, globalized (in-)security and sociotechnical visions of the digital society", *Österr. Z. Für Soziol.*, vol. 44, nr. 1, pp. 115–134, iun. 2019, doi: 10.1007/s11614-019-00350-7.
25. S. Peng, „Digital economy and national security: contextualizing cubersecurity-related exceptions", *AJIL UNBOUND*, vol. 117, pp. 122–127, mai 2023, doi: 10.1017/aju.2023.18.
26. V. Petrov, „Establishing a national cybersecurity system in the context of national security and defence sector reform", *Inf. Secur.*, vol. 31, nr. 1, pp. 73–77, 2014, doi: 10.11610/isij.3004.
27. G. R. Ivanov, „The cybersecurity of automated control systems as a key conponent of national security", *J. Def. Resour. Manag.*, vol. 7, nr. 2, pp. 91–96, 2016.
28. Eviatar Matania, L. Yoffe, și M. Mashkautsan, „A Three-Layer Framework for a Comprehensive National Cyber-security Strategy", *Georget. J. Int. Aff.*, vol. 17, nr. 3, pp. 77–84, Winter 2016, doi: 10.1353/gia.2016.0038.
29. D. Štitilis, P. Pakutinskas, și I. Malinauskaitė, „EU and NATO cybersecurity strategies and national cyber security strategies: a comparative analysis", *Secur. J.*, vol. 30, nr. 4, pp. 1151–1168, 2017, doi: DOI:10.1057/s41284-016-0083-9.
30. E. Dolzhenkova, D. Mokhorov, și T. Baranova, „National and International Issues of Cyber Security", *IOP Conf. Ser. Mater. Sci. Eng.*, 2020, doi: 10.1088/1757-899X/940/1/012015.

31. R. Piotrowski și J. Sliwa, „Cyberspace situational awarness in national security system", în *2015 International Conference on Military Communications and Information Systems (ICMCIS)*, mai 2015, pp. 1–6. doi: 10.1109/ICMCIS.2015.7158685.
32. A. Gilad, E. Pecht, și A. Tishler, „Intelligence, Cyberspace, and National Security", *Def. Peace Econ.*, vol. 32, nr. 1, pp. 18–45, ian. 2021, doi: 10.1080/10242694.2020.1778966.
33. Z. Ciekanowski, M. Gruchelski, J. Nowicka, S. Żurawski, și Y. Pauliuchuk, „Cyberspace as a Source of New Threats to the Security of the European Union", *Eur. Res. Stud. J.*, vol. XXVI, pp. 782–797, sep. 2023, doi: 10.35808/ersj/3249.
34. P. Yannakogeorgos și A. Lowther, *Conflict and Cooperation in Cyberspace: The Challenge to National Security*. 2013.
35. S. Garibaldi și F. Deane, „Cyberspace as a fifth dimension of national security: trade measure exceptions", *J. Int. Trade Law Policy*, vol. 22, pp. 67–88, iun. 2023, doi: 10.1108/JITLP-01-2023-0004.
36. M. Moore, „Development and Implementation of Government Cybersecurity Policies and Practices for National Security and Cybercrime", 2014.
37. E. P. Petrescu și F. L. Giusca, „Threats if cybercrime in the field of economic and financial security at national and regional level", *Int. Sci. Conf. Strateg. XXI Suppl Strateg. Chang. Secur. Int. Relat.*, vol. 3, pp. 150–154, 2018.
38. I. Apachiței și C. Ichim, „The implications of cybercrime for national security", *SHS Web Conf.*, vol. 177, sep. 2023, doi: 10.1051/shsconf/202317703003.
39. A. Tulvan și G. Panfil, „The importance of education related to cyber crimes in the traininf institution dedicated to public order and national secutiry - a case study focused on Romanian Ministry of Internal Affairs", prezentat la ELEARNING VISION 2020!, VOL I, I. Roceanu, D. Dubois, F. Moldoveanu, I. Stanescu, D. Beligan, M. Dascalu, și D. Barbieru, Ed., 2016, pp. 481–484. doi: 10.12753/2066-026X-16-069.
40. E. M. Ngwana, „Emerging Paradigms of Cybercrimes, Supply Chain Attacks, and National Security Ramifications", D.Sc., Marymount University, United States -- Virginia, US, 2022. [Online]. Disponibil la: https://www.proquest.com/dissertations-theses/emerging-paradigms-cybercrimes-supply-chain/docview/2817856379/se-2?accountid=15533
41. N. Varenia, I. Avdoshyn, L. Strelbytska, M. Strelbytskyy, și M. Palchyk, „Cybercrime as a threat to Ukreaine's national security", *Int. J. Comput. Sci. Netw. Secur.*, vol. 21, nr. 5, pp. 73–83, mai 2021, doi: 10.22937/IJCSNS.2021.21.5.13.
42. T. Gudu, „A logic model for the national cyber security / defence strategies? The case of French cuber defence pact", *Int. Sci. Conf. Strateg. XXI*, vol. 3, pp. 156–161, 2016.
43. E.-V. Popa, „Aspects of national policy to ensure cyber security and defense in France and Germany", *Int. Sci. Conf. Strateg. XXI Suppl Strateg. Chang. Secur. Int. Relat.*, vol. 3, pp. 155–160, 2018.
44. H. Kaponig, „Austria's National Cyber Security and Defense Policy: Challenges and the Way Forward", *Connect. Q. J.*, vol. 19, nr. 1, pp. 21–37, Winter 2020, doi: 10.11610/Connections.19.1.03.
45. D. Dumitru și G. C. Iuhas, „Cyber security - a new dimension of national defense", *Int. Sci. Conf. Strateg. XXI Suppl Technol. - Mil. Appl. Simul. Resour.*, vol. 1, pp. 176–182, 2018.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.