*European Research Studies Journal*
*Volume XXVI, Issue 3, 2023*

*pp. 782-797*

# Cyberspace as a Source of New Threats to the Security of the European Union

*Submitted 01/08/23, 1st revision 13/08/23, 2nd revision 18/09/23, accepted 30/09/23*

Zbigniew Ciekanowski[1], Marek Gruchelski[2], Julia Nowicka[3], Sławomir Żurawski[4], Yury Pauliuchuk[5]

***Abstract:***

***Purpose:*** *The main aim of this article is to characterize threats in the cyber domain affecting the security of European Union (EU) member states.*
***Design/Methodology/Approach:*** *The primary research question is formulated as follows: Does the European Union play a significant role in shaping cybersecurity? Correspondingly, the hypothesis adopted to address the research question is as follows: The EU takes actions to enhance resilience against cyberattacks. In the initial section of the article, fundamental concepts of cyber security and cyberspace are defined. Subsequently, EU tools, Union legal regulations, as well as the obligations of key entities pertaining to cyber threats are presented. The main part of the article provides a detailed characterization of new and major threats to EU member states*
***Findings:*** *The European Union plays a significant role in shaping European cybersecurity, primarily through legislation and its subordinate institutions, which are intended to prevent and rapidly and effectively respond to emerging and new cyber threats.*
***Practical implications:*** *The study relies on the latest research presented in documents and reports in the field of cybersecurity, published between 2020-2022 by international organizations. Additionally, an analysis is conducted based on recent scholarly articles. Information is also sourced from national legal acts and documents published by European Union authorities.*
***Originality/Value:*** *This article addresses security management issues related to the field of cybersecurity, which constitutes a new challenge in light of the rapid development of technology and emerging cyber threats in cyberspace.*

***Keywords:*** *Cyber threats, cybersecurity, European Union, sector, organization, management.*
***JEL codes:*** *F52, H5, K24, M10.*
***Paper type:*** *Research article.*

[1] *Faculty of Economics, John Paul  II Univerrsity of Applied Sciences in Biała Podlaska, Poland, ORCID: 0000-0002-0549-894X,  zbigniew@ciekanowski.pl;*
[2] *Warsaw Management University, Poland, ORCID: 0000-0003-4177-1613, gruchelscy@tlen.pl;*
[3] *War Studies University, Poland, ORCID: 0000-0002-0778-0519, j.nowicka@akademia.mil.pl;*
[4] *State School of Higher Education in Chełm, Poland, ORCID: 0000-0001-9527-3391, slawomir.zurawski@onet.pl;*
[5] *Siedlce University of Natural Sciences and Humanities, Poland, ORCID:  0000-0002-2077-5124, y.pauliuchuk@wp.pl;*

## 1. Introduction

Cyberspace is expanding year by year, and its impact on human life is becoming increasingly evident. Proper protection of all processes that can adversely affect human life is therefore an essential element that should accompany the rapid development of telecommunications. A secure cyberspace is also closely linked to the internal and external security of every country. Preparing appropriate international security guarantees in cyberspace is a major challenge for every nation.

The European Union and the Council of Europe should be leaders in this regard. The absence of legal regulations and standards regarding a secure cyberspace creates the possibility of exposing society to the takeover of their privacy, data theft, or other crimes that carry serious consequences.

Therefore, the introduction of European norms that should apply in every country is a crucial element. The coordination of security systems, including those related to cyberspace, should provide a future perspective ensuring an adequate level of security for citizens against cyber threats.

## 2. The Definition of Cyberspace and Cybersecurity Concepts

In contrast to the concept of cybersecurity, the concept of cyberspace does not have one universally accepted and agreed-upon definition. Due to its dynamically changing nature, it leads to both interpretational and definitional difficulties. The term "cyberspace" first appeared in William Gibson's science fiction novel "Neuromancer." The book was set in an imaginary space constructed from processes of electronic communication (Dobrzeniecki, 2004).

Cyberspace is considered from various perspectives. From a psychological point of view, it is defined as a state of mind. John P. Barlow asserts that cyberspace is "any space in which people can gather their minds without bringing their bodies there" (Dobrzeniecki, 2004). According to Pierre Levy's concept, cyberspace is "a space of open communication through interconnected computers and computer memories operating worldwide."

However, cyberspace cannot be equated solely with the Internet. It has a broader character; it is the space of human digital activity but largely relies on the Internet (Wrona, 2017). As stated in the American National Strategy to Secure Cyberspace, cyberspace has become the "nervous system of the state": "(...) our economy and national security have become fully dependent on technology and information infrastructure" (The White House, 2003).

The efficiency and security of cyberspace are essential for the functioning of critical infrastructure (The White House, 2011), and consequently, for the security of the entire nation and its citizens. On the other hand, the concept of "cybersecurity" derives from the term "information security," but it is used in reference to a wider range of issues, also related to national security (RAND, 2015). It should be noted that a single coherent and universal definition of cybersecurity for all environments has not been created (Chmielewski, 2016).

To begin discussions on EU cybersecurity, it is necessary to present the definition of cybersecurity that was applicable at the time and is currently in legal acts of the community. In EU documents, it is stated that cybersecurity generally refers to measures and actions that can be used to protect the cyber domain, both civil and military, from those threats that concern its interdependent networks and information infrastructure and that can damage these networks and infrastructure (JOIN(2013) 1 final – 7.2.2013).

"Cybersecurity means actions necessary to protect networks and information systems, users of such systems, and other persons from cyber threats" (Regulation (EU) 2019/881). In the UK's National Cyber Strategy 2022, it is stated that Cyberpower, or Cyber Strength, is the ability to protect national interests in cyberspace, as well as beyond it. Countries that excel in navigating the opportunities and meeting challenges will be safer and more resilient to threats in cyberspace in the future (HM Government, 2022).

## 3. The EU in the Fight Against Cyber Threats

In recent times, society has gained a greater awareness of the negative aspects of the widespread use of the Internet. Cyberspace is not only a place where people work, acquire knowledge, communicate with each other, or seek entertainment, but it is also an area in which people are exposed to various threats (Tadeusiewicz, 2010).

Continuing the discussion on cybersecurity in Europe, it is necessary to trace back to the early stages of defining threats in cyberspace in international law. In this legal domain, the Council of Europe made the first attempt in 2001 in Budapest when it adopted the Convention on Cybercrime (the Budapest Convention), which defines specific concepts as follows:

a) "computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic data processing;
b) "computer data" means any representation of facts, information, or concepts in a form suitable for processing in a computer system, including the corresponding program that causes the execution of functions by the computer system;
c) "service provider" means any private or public entity that enables users of its services to communicate through a computer system and any other entity that processes or stores computer data on behalf of such communication services or users of such services;

d) "traffic data" means any computer data relating to communication through a computer system, generated by the computer system that formed a part of the communication chain, indicating the origin, destination, route, time, date, size, duration, or type of a given service (Journal of Laws 2015, item 728).

In order to achieve a high level of cybersecurity, cyber resilience, and trust within the European Union, Regulation (EU) 2019/881 was introduced concerning ENISA (the European Union Agency for Cybersecurity) and cybersecurity certification of information and communication technology (ICT) products (the Cybersecurity Act). The EU Cybersecurity Act came into effect in June 2019 and introduced, among other things, a comprehensive EU certification program and a strengthened mandate for the EU Agency for Cybersecurity.

The EU framework for the certification of cybersecurity of ICT products enables the development of tailored and risk-based EU certification programs. Certification plays a significant role in enhancing trust and security in the cyber domain. Within the EU, there are various cybersecurity product certification systems in place. However, without common frameworks for cybersecurity certificates valid across the entire EU, there is a growing risk of fragmentation and barriers between member states.

From the above, it follows that each European system should define:

a) The categories of covered products and services.
b) Cybersecurity requirements, such as standards or technical specifications.
c) The type of assessment, e.g., self-assessment or third-party assessment.
d) The intended level of assurance.

To attain a high level of cybersecurity, cyber resilience, and trust within the European Union (EU), Regulation (EU) 2019/881 was enacted concerning ENISA (the European Union Agency for Cybersecurity) and the certification of cybersecurity for information and communication technology (ICT) products (the Cybersecurity Act).

The EU Cybersecurity Act came into effect in June 2019, introducing, among other things, a comprehensive EU certification program and a strengthened mandate for the EU Agency for Cybersecurity.

The obtained certificate will be recognized in all EU member states, facilitating cross-border trade for businesses and providing consumers with a better understanding of product or service security (European Commission, 2023). Notably, the new EU Agency for Cybersecurity is built upon the structures of its predecessor, the Agency for the European Union for Network and Information Security (ENISA), but it has gained a more prominent role and a permanent mandate. It continues to operate under the acronym ENISA, supporting EU member states, EU institutions, and other stakeholders in dealing with cyber threats.

Another element in European cybersecurity is the European Defence Agency (EDA), with which the EU collaborates in the field of defense in cyberspace. EDA undertakes joint actions with the EU Agency for Cybersecurity and Europol. EDA supports EU member states in training qualified military personnel involved in cyber defense and ensures the availability of proactive and reactive cybersecurity technologies (European Council, 2023).

The realm of network and information systems security, stemming from efforts to advance the digital society and market, is regulated by the Directive of the European Parliament and of the Council (EU) 2016/1148 on measures for a high common level of network and information systems security (JOIN(2017) 450 final), adopted on July 6, 2016 (the NIS Directive).

This directive outlines the security obligations for operators of essential services (in critical sectors such as energy, transportation, health, and finance) and digital service providers (online marketplaces, search engines, cloud services). In December 2020, the European Commission proposed to replace the 2016 directive with an amended directive (NIS2) in response to evolving threat landscapes and the digital transformation accelerated by the COVID-19 crisis.

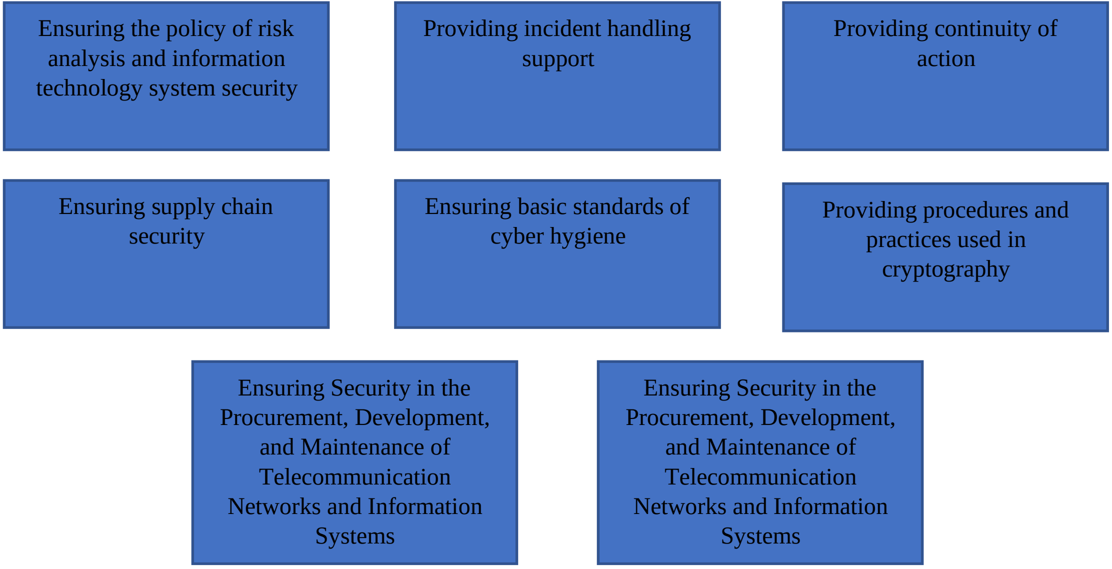
A preliminary agreement on the proposed directive was reached by the European Council and the European Parliament in May 2022. The new regulations will enhance risk management, incident handling, and expand the directive's scope.

The Directive on measures for a high common level of cybersecurity throughout the Union (NIS2 Directive) envisions legal measures aimed at increasing the overall level of cybersecurity in the EU by ensuring:

a) Preparedness of member states, requiring them to be adequately equipped. For example, through the cooperation of Computer Security Incident Response Teams (CSIRTs) and competent national authorities responsible for network and information systems (NIS).
b) Cooperation among all member states through the establishment of a cooperation support group, facilitating strategic cooperation and information exchange among member states.
c) A culture of security in all sectors critical to the economy and society, largely reliant on information and communication technologies, such as energy, transportation, water, banking, financial market infrastructure, healthcare, and digital infrastructure (Directive (EU) 2022/2555).

NIS 2 also imposes new reporting obligations on entities. According to the proposal, reporting will encompass not only information and communication technology incidents but also "any significant cyber threat." Figure 1 illustrates selected obligations of entities under the NIS 2 directives.

***Figure 1.*** *Obligations of Key and Important Entities.*


Ensuring the policy of risk analysis and information technology system security
Providing incident handling support
Providing continuity of action
Ensuring supply chain security
Ensuring basic standards of cyber hygiene
Providing procedures and practices used in cryptography
Ensuring Security in the Procurement, Development, and Maintenance of Telecommunication Networks and Information Systems
Ensuring Security in the Procurement, Development, and Maintenance of Telecommunication Networks and Information Systems

***Source:*** *Compiled based on Directive (EU) 2016/1148 of the European Parliament and of the Council on measures for a high common level of network and information systems security.*

The NIS 2 Directive applies to key entities and important sectors, typically including at least medium-sized businesses. Key and important entities share similar obligations, but these obligations are to be applied proportionally, taking into account the specific characteristics of each entity. The primary obligations of key and important entities include implementing cybersecurity risk management measures and reporting serious incidents (Szczęsna, 2022).

In Poland, the NIS Directive is implemented into law through the National Cybersecurity System Act of July 5, 2018 (Journal of Laws 2018, item 1560). In the latest amendment proposal from March 25, 2022, measures such as the procedure for designating a provider as a high-risk provider have been suggested, and the introduction of national cybersecurity certification programs has been announced.

The scale and level of cyberattacks and cybercrime are on the rise across Europe. Experts predict that this trend will continue to intensify, with projections indicating that by 2025, as many as 41 billion devices worldwide will be connected to the Internet. Adequate cybersecurity policies and decisive actions can enhance the level of security and trust citizens have in digital tools and services.

The EU's cybersecurity policy is built upon four main pillars:

1. **Joint actions for stronger EU cybersecurity:** The EU aims to enhance its coordination mechanisms between national and EU entities involved in cybersecurity to increase the exchange of information and cooperation between military and civilian communities involved in cybersecurity, as well as to further support Common Security and Defence Policy (CSDP) missions and operations.
2. **Securing the EU defense ecosystem:** Even non-critical software components can be exploited for cyberattacks on businesses or governments, including in the defense sector. This necessitates further work on standardization and cybersecurity certification to secure both military and civilian domains.
3. **Investing in cyber defense capabilities:** EU member states are required to significantly increase investments in modern military cyber defense capabilities in a cooperative manner, utilizing cooperation platforms and funding mechanisms available at the EU level, such as the Permanent Structured Cooperation (PESCO), European Defence Fund, Horizon Europe, and Digital Europe program.
4. **Partnerships in addressing common challenges:** Building on existing security and defense dialogues and cyber discussions with partner countries, the EU will seek to establish tailored partnerships in the field of cyber defense (European Commission, 2022).

The European Union's engagement in cybersecurity policy is undeniable. This is evident not only from the analysis of debates taking place within the cooperation between institutions and member states but also internally among EU institutions themselves. It is also reflected in research on EU secondary law acts (Małecka, 2021).

A fundamental principle of EU institutions is the creation of secondary law within the clearly defined competencies laid out in the treaties (Małecka, 2021). The Treaty on the Functioning of the European Union, in particular, serves as the legal basis for the operation of EU law. The area of freedom, security, and justice is governed by shared competencies between the Union and member states (Kuś, 2014).

Member states can only legislate in this area when the Union does not exercise its competence or decides to discontinue it. Cybersecurity is one of the avenues through which the Union can pursue its strategic goals, transforming itself into a strong player in international relations, expanding its activities beyond the economic domain into the realm of defense (Małecka, 2021).

## 4. Cybersecurity: The Main and New Threats

In the context of cybersecurity threats concerning the European Union, there exists a necessity to refer to a catalogue of issues that should be regulated by cyber security policy. Analyzing foreign-language literature, one can delineate a catalogue of issues related to cybersecurity, which includes:

a) Matters pertaining to the multi-faceted and multi-entity governance of the cyber domain (net neutrality in the electronic communications market, allocation of names and addresses on the Internet, copyright and trademarks, unsolicited email correspondence).
b) Issues related to cyberspace users: actions involving malicious software in advertisements (malvertising), impersonation, responsible usage, cybercrime, geolocation, and privacy.
c) Matters associated with cyber conflicts (including theft of intellectual property, cyber espionage, cyber sabotage, cyber warfare).
d) Challenges associated with cyber infrastructure.
e) Detailed cyber space management issues (such as responsibility for entrusted data, risk management, professional certification, security principles, research, and development) (Bayuk, 2012).

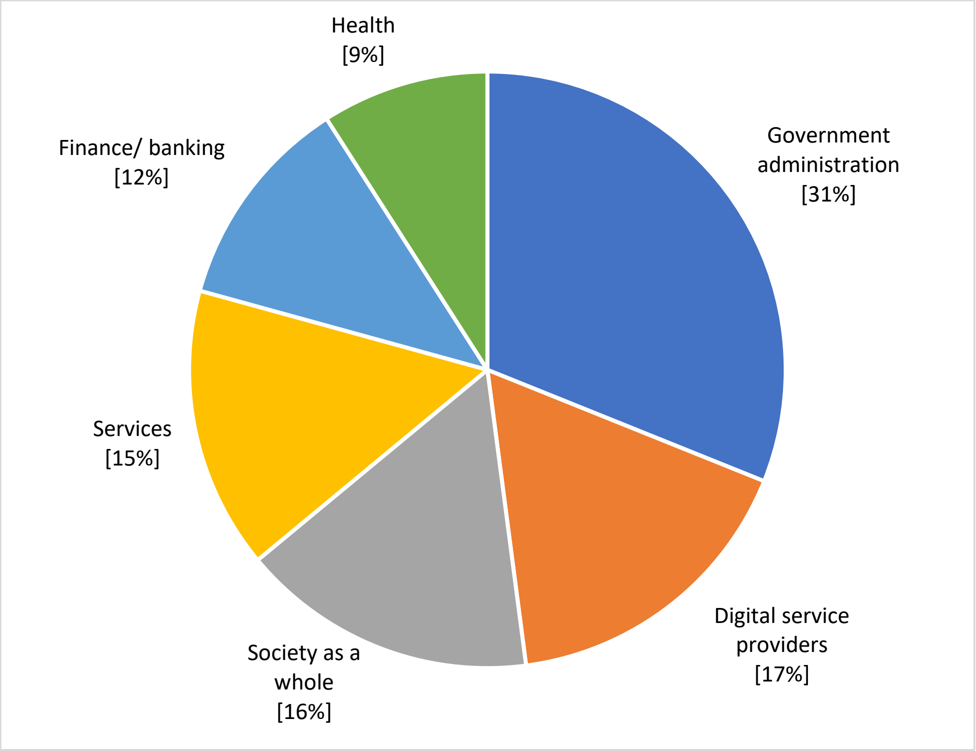
Cyber threats typically do not confine themselves to specific sectors and, in most cases, affect more than one area. Various factors contribute to threats manifesting as incidents in specific sectors, making it crucial to deeply examine the sectoral aspects of observed incidents and threats. Cyber threats in the European Union impact key sectors (ENISA, 2022).

The volume of reported incidents underscores the need for streamlining the incident reporting process in the EU, which is reflected in the NIS 2 Directive. In this regard, the ENISA Agency will continue its efforts in the coming years. To this end, the following impact types have been defined:

a) Reputation impact, which pertains to the potential negative publicity or negative public perception of an entity that has fallen victim to a cyber incident.
b) Digital impact, which relates to damaged or inaccessible systems, compromised data files, or data exfiltration.
c) Economic impact, which refers to direct financial losses, damage to national security resulting from the loss of critical materials, or ransom payments.
d) Physical impact, which encompasses any injuries or harm caused to employees, customers, or patients.
e) Social impact, which concerns any influence on society as a whole or widespread disruptions that can affect society (e.g., incidents disrupting the national healthcare system in a given country) (ENISA, 2022).

Figure 2 illustrates six sectors most affected by cyber threats from June 2021 to June 2022.

***Figure 2.*** *The main sectors affected by cyberthreats*



***Source:*** *ENISA, 2022.*

In the presented Figure, a significant number of incidents can be observed targeting public administration, government, and digital service providers. The high incidence of attacks on digital service providers is expected due to their horizontal provision of services to this sector, consequently affecting many other sectors. Meanwhile, the financial sector experienced a consistent number of incidents throughout the entire period, with the healthcare sector closely following.

The use of the Internet and the free flow of information have an impact on the lives of every individual. For many people, access to the Internet has become a fundamental necessity for work, education, exercising freedom of expression, political freedoms, and social interactions. As a result, the increasing number of users and the frequency of usage contribute to the emergence of new threats.

According to Juhan Lepassaar, Executive Director of ENISA, "*Future threats cannot be postponed or avoided. Therefore, any insight into the future is our best security plan - in line with the proverb 'prevention is better than cure.' It is our duty to take every possible measure as early as possible to increase our resilience over the years and contribute to improving cyber security in 2030 and beyond.*"

A substantial quantity of threats within the cyber domain emerged during the years 2021 and 2022. Drawing upon the analysis presented in the ENISA Threat Landscape 2022 report, the agency identifies and focuses on the following eight principal threat categories:

1. **Ransomware**, defined according to the ENISA Threat Landscape for Ransomware Attacks report as a type of attack wherein cybercriminals seize control of target resources and demand ransom in exchange for restoring resource availability.

2. **Malware**, also referred to as malicious code and malicious logic (NIST, 2019), is the overarching term used to describe any software or hardware designed to execute unauthorized processes that will adversely affect the confidentiality, integrity, or availability of a system.

3. **Social engineering** encompasses a wide range of activities that seek to exploit human error or behavior to gain access to information or services (NIST, 2020). It employs various forms of manipulation to induce victims into making errors or divulging sensitive or confidential information. In the realm of cybersecurity, social engineering persuades users to open documents, files, or email messages, visit websites, or grant unauthorized individuals access to systems or services.

4. **Data threats** constitute a collection of perils directed at data sources with the aim of obtaining unauthorized access, disclosure, and manipulation of data to interfere with system behavior. These threats also serve as the foundation for numerous other threats discussed within this report. For example, ransomware, RDoS (Ransomware Denial of Service), and DDoS (Distributed Denial of Service) seek to deny access to data and potentially demand payment for its restoration.

5. **Threats to availability**, such as Denial of Service (DoS), are a prime focus. Availability is the target of numerous threats and attacks, with DDoS prominently featured among them. DDoS attacks compromise system and data availability and, while not a novel threat, play a significant role in the cybersecurity threat landscape (Imperva, 2023). These attacks occur when system users or services are denied access to essential data, services, or other resources (Europol, 2020). This can be achieved through service exhaustion or overloading of network infrastructure components (CISA, 2021).

6. **Availability threats: Internet threats.** The use of the Internet and the free flow of information have a profound impact on the lives of individuals. For many, Internet access has become a fundamental necessity for work, education, and the exercise of freedom of speech, political liberty, and social

interaction. This category encompasses threats affecting Internet availability, such as BGP (Border Gateway Protocol) interception.

7. **Disinformation campaigns** continue to intensify, driven by the increasing use of social media platforms and online media. Digital platforms have become the norm for news and media consumption. Social networking sites, news services, media outlets, and even search engines now serve as sources of information for many individuals.

8. **Supply chain attacks** target the relationships between organizations and their suppliers (ENISA, 2021). According to the definition provided in the ENISA Threat Landscape for Supply Chain document, an attack is considered to involve a supply chain element if it comprises a combination of at least two attacks.

After an 8-month forecasting exercise, ENISA identified and ranked the 10 major cyber security threats expected to emerge by 2030. Supported by a panel of experts from ENISA's forecasting group, CSIRT networks, and EU CyCLONe experts, ENISA conducted a panel discussion during threat identification workshops to explore solutions for emerging challenges in the perspective of 2030 (ENISA, 2022). Figure 3 illustrates the ten top cyber threats forecasted by ENISA that may emerge by 2030.

***Figure 3.*** *ENISA Threat Landscape 2022 - Major Threats*

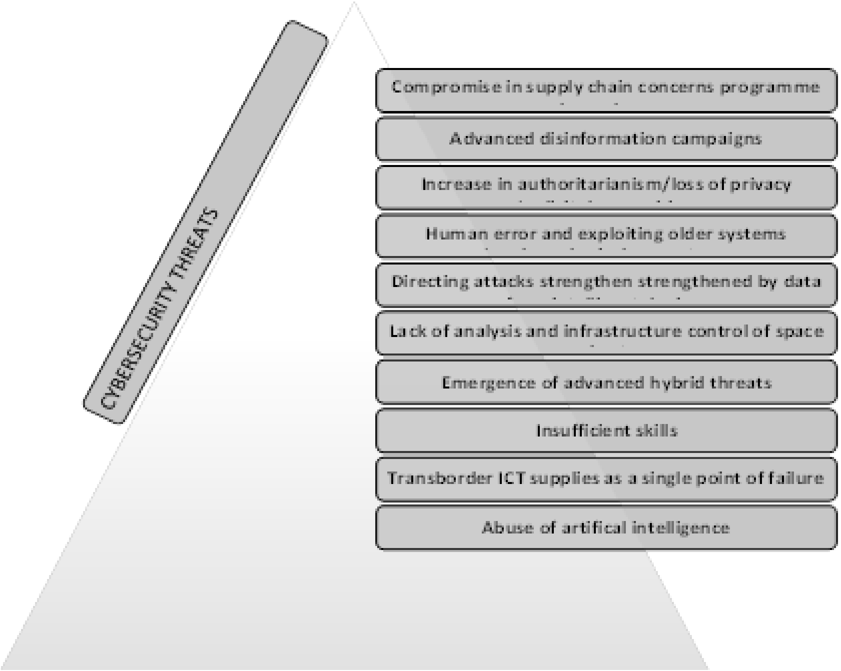
| **PROXIMITY** | **FEARS** |
|---|---|
| **CLOSE** | The affected networks, systems, controlled, and secured within the EU boundaries. The affected population within the EU boundaries. |
| **MEDIUM** | The networks and systems deemed critical for operational purposes within the framework of the EU's Digital Single Market and NIS Directive sectors, but their control and assurance rely on institutional or public bodies, or private entities outside the EU, within the member states. The affected population in geographic areas near the EU borders. |
| **DISTANT** | The networks and systems that, if influenced, will have a critical impact on operational objectives within the scope of the EU's Digital Single Market and NIS Directive sectors. The control and assurance of these networks and systems are beyond the competence of EU institutional bodies or public and private entities within member states. The affected population suffering from the disease is located in geographic areas distant from the EU. |
| **GLOBAL** | All aforementioned areas. |

***Source:*** *Adapted from ENISA Threat Landscape 2022*

It should be noted that the mentioned threats are categorical in nature and pertain to a set of different threat types consolidated into the eight areas listed above. An important aspect to consider in the context of the ENISA Threat Landscape is the proximity of cyber threats in relation to the European Union. This is a significant element to aid analysts in assessing the significance of cyber threats.

According to the proposed classification for the EU's Common Security and Defense Policy (European Parliamentary Research Service, 2019), the classification of cyber threats encompasses four categories. The threat proximity classification is presented in Table 1.

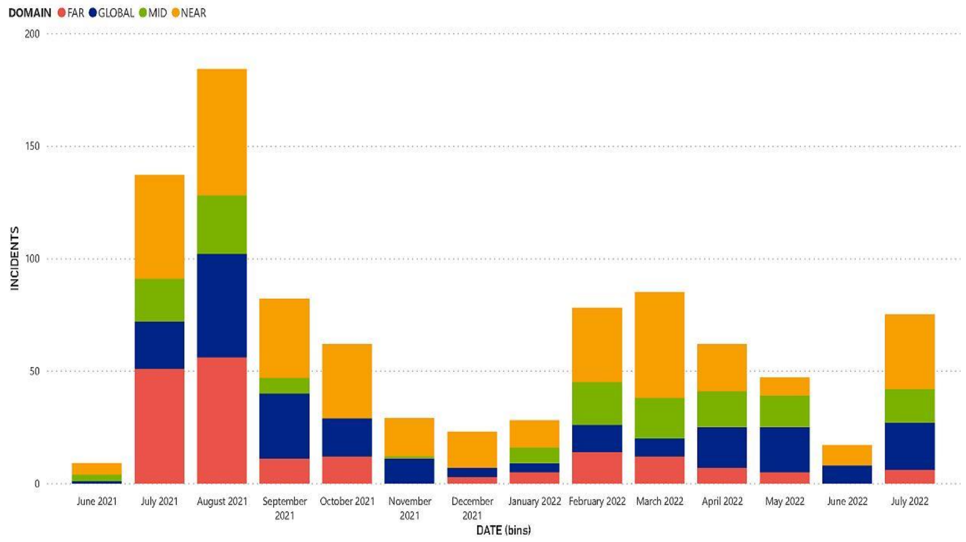
***Table 1.*** *Classification of Threat Proximity*


CYBERSECURITY THREATS
Compromise in supply chain concerns programme
Advanced disinformation campaigns
Increase in authoritarianism/loss of privacy
Human error and exploiting older systems
Directing attacks strengthen strengthened by data
Lack of analysis and infrastructure control of space
Emergence of advanced hybrid threats
Insufficient skills
Transborder ICT supplies as a single point of failure
Abuse of artifical intelligence

***Source:*** *ENISA, 2022.*

Figure 4 depicts a time series of incidents related to the main threat categories reported in ETL 2022. It is worth noting that the information on the chart is based on OSINT (Open Source Intelligence) and is the result of ENISA's situational awareness efforts.

***Figure 4.*** *Observed Incidents Related to ETL's Main Threats (OSINT-based Situational Awareness) in Terms of Their Proximity*



***Source:*** *ENISA, 2022.*

As evident from the above chart, in the year 2022, there was a generally lower number of incidents in comparison to 2021. Specifically, the category "NEAR," denoting proximity, exhibits a consistent and high number of observed incidents associated with major threats, implying their significance within the context of the European Union (EU). This outcome is unsurprising given the geopolitical situation in which the EU finds itself.

During the latter half of 2021 and throughout 2022, the number of cyberattacks continued to rise, not only in terms of vectors and quantities but also in terms of their consequences. The Russo-Ukrainian crisis ushered in a new era for cyber warfare and activism, redefining their roles and impact on conflicts. States and other cyber actors are highly likely to adapt to this new reality and capitalize on the novelties and challenges that this war brings with it (Council on Foreign Relations, 2022).

Hence, the analysis and characterization of both existing and emerging threats assume exceptional importance within the realm of cybersecurity. A sound and coherent international policy will ensure the minimization of threats adversely affecting the security of the state and its citizens.

## 5. Conclusions

The optimal structure of international security guarantees in cyberspace is a challenge that must be a priority for all states seeking to protect their citizens from cyber threats. The contemporary challenges in the field of cybersecurity include the necessity of international cooperation, the development of collaborative methods, and the formulation of new legal regulations.

Recently, the European Union (EU) has recognized that cybersecurity and associated threats constitute a major challenge for the security policy of the community. This is evident in the adoption of increasingly ambitious strategies, the establishment of new organizations, and the implementation of regulations aimed at countering cyber threats. Existing regulations and actions of individual EU institutions responsible for cybersecurity collectively create an effective European system for safeguarding the citizens, businesses, and public institutions of Europe in this regard.

However, it is important to note that as a result of successful and visible law enforcement efforts, cybercriminals may intensify their efforts in developing more effective methods and tools for cyberattacks. The EU is taking steps to enhance resilience against cyberattacks, thus playing a significant role in shaping European cybersecurity.

This is primarily achieved through legislation and its subordinate institutions, which are designed to prevent and respond swiftly and effectively to emerging and new cyber threats. Taking the above into consideration, the hypothesis put forward has been confirmed.

## References:

Bayuk, J.L., Healey, J., Rohmeyer, P., Sachs, M.H., Schmidt, J., Weiss J. 2012. Cyber Security Policy Guidebook, John Wiley & Sons Inc., Hoboken, New Jersey.

Chmielewski, Z. 2016. Polityka publiczna w zakresie ochrony cyberprzestrzeni w UE i państwach członkowskich, „Studia z polityki publicznej”, nr 2(10)2016.

CISA. 2021. Understanding Denial-of-Service Attacks, https://www.cisa.gov/news-events/news/understanding-denial-service-attacks.

Council Foreign Relations. 2022. Cyber Proxies in the Ukraine Conflict: Implications for International Norms, https://www.cfr.org/blog/cyber-proxies-ukraine-conflict-implications-international-norms.

RAND. 2015. Cybersecurity in the European Union and Beyond: Exploring the Threats and Policy Responses, Directorate – General for Internal Policies, Brussels.

Dobrzeniecki, K. 2004. Prawo a etos cyberprzestrzeni, Wydawnictwo Adam Marszałek, Toruń.

Dyrektywa (UE) 2016/1148 Parlamentu Europejskiego i Rady w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych, https://eur-lex.europa.eu.

Dyrektywa (UE) 2022/2555 Parlamentu Europejskiego i Rady z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2), https://eur-lex.europa.eu.

European Parliamentary Research Service. 2017. Cybersecurity in the EU Common Security and Defence Policy (CSDP). Challenges and risks for the EU. https://www.europarl.europa.eu/RegData/etudes/STUD/2017/603175/EPRS_STU(2017)603175_EN.pdf.

Europol. 2020. Ocena zagrożenia przestępczością zorganizowaną w Internecie (IOCTA) 2020. https://www.europol.europa.eu/publications-events/main-reports.

ENISA. 2021. Threat Landscape for Supply Chain Attacks. https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks.

ENISA. 2022. Cybersecurity Threats Fast-Forward 2030: Fasten your Security-Belt Before the Ride! https://www.enisa.europa.eu/news/cybersecurity-threats-fast-forward-2030.

ENISA. 2022. ENISA Threat Landscape 2022. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022.

ENISA. 2022. ENISA Threat Landscape for Ransomware Attacks. https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-ransomware-attacks.

Imperva. 2023. What is Social Engineering – Attack Techniques & Prevention Methods, https://www.imperva.com/learn/application-security/social-engineering-attack/.

Kuś, A.  2014. Rodzaje kompetencji Unii Europejskiej a unijna polityka podatkowa. Studia z Polityki Publicznej, nr 2(2).

Komisja Europejska. 2022. Polityka Unii Europejskiej w zakresie obrony cyberprzestrzeni, https://ec.europa.eu/commission/presscorner/detail/en/ip_22_6642.

Komisja Europejska. 2023. Unijne ramy cyberbezpieczeństwa. https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-certification-framework.

Konwencja Rady Europy o cyberprzestępczości, sporządzona w Budapeszcie dnia 23 listopada 2001 r. (Dz.U. 2015 poz. 728.)

Małecka, A. 2021. Polityka cyberbezpieczeństwa Unii Europejskiej na początku trzeciej dekady XXI wieku. Rocznik Bezpieczeństwa Międzynarodowego, vol. 15, nr 2.

HM Government. 2022. National Cyber Strategy 2022. Pioneering a cyber future with the whole of the UK. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1053023/national-cyber-strategy-amend.pdf.

NIST. 2019. Malware – Glossary. https://csrc.nist.gov/glossary/term/malware.

NIST. 2020. Protecting Controlled Unclassified Information in Nonfederal Systems. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf.

Rada Europejska. 2023. Cyberbezpieczeństwo: jak UE radzi sobie z cyberzagrożeniami. https://www.consilium.europa.eu/pl/policies/cybersecurity/#defence.

Rozporządzenie (UE) 2019/881 Parlamentu Europejskiego i Rady z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie) (Tekst mający znaczenie dla EOG). https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A32019R0881.

Szczęsna, A. 2022. Obowiązki podmiotów kluczowych i ważnych w Dyrektywie NIS 2. https://cyberpolicy.nask.pl/obowiazki-podmiotow-kluczowych-i-waznych-w-dyrektywie-nis2/.

Tadeusiewicz, R. 2010. Zagrożenia w cyberprzestrzeni. Nauka, nr 4/2010.

The White House. 2011. International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World. http://www.hsdl.org/?view&did=5665.

The White House. 2003. The National Strategy to Secure Cyberspace. https://www.hsdl.org/c/view?docid=1040.

Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, Dz.U. 2018 poz. 1560.

Wrona, J. 2017. Cybeprzestrzeń a prawo międzynarodowe. Status quo i perspektywy, Uniwersytet w Białymstoku, Białystok.

Wspólny Komunikat do Parlamentu Europejskiego. Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów - Strategia bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń (JOIN(2013) 1 final – 7.2.2013). https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:52013JC0001.

Wspólny Komunikat Komisji do Parlamentu Europejskiego i Rady, Odporność, prewencja i obrona: budowa solidnego bezpieczeństwa cybernetycznego (JOIN(2017) 450 final). https://eur-lex.europa.eu/legal-content/EN/TXT/?qi d=1505294563214&uri=JOIN:2017:450:FIN.