Elżbieta Hodyr
War Studies University
ORCID: 0000-0001-5045-093X
e-mail ehodyr@gmail.com

Cybersecurity in NATO and the European Union

Abstract I'm writing this article to expand and organize my knowledge of cybersecurity. My interests include cybersecurity in NATO and the EU. I'd like to compare cybersecurity in both organizations and how the organizations within NATO and the EU responsible for cybersecurity operate. I'd like to address the strategic challenges regarding cybersecurity in NATO and the EU. I'd also like to describe the cybersecurity of diplomatic missions in connection with the war in Ukraine.

Key words cybersecurity, NATO, EU, strategy, diplomatic mission, cooperation

Introduction

In the beginning, what is cybersecurity? Cybersecurity comprises three planes of study: operations address the day-to-day functioning of the information security tasks. Operational issues included staffing, implementation of policies and procedures, incident response, business continuity, disaster recovery, systems management, tool acquisition and deployment, investigations and more.

Governance function includes the development of organizational structure and command chain that oversees, manages and handles information and information systems. Governance include the development of policies and procedures that drive the operational aspects, the laws and policies that set the

societal expectations of individual and organization activities. Categories of law include criminal law (statutes guiding actions that are deemed to threaten harm public safety or welfare), civil law and administrative law.

Training refers to teaching individuals specific skills and competencies that are usually task-or project-oriented[1]. Cybersecurity is also a concept that refers to ensuring protection and counteracting threats that affect cyberspace itself and the functioning of cyberspace, and this applies to both the public and private sectors and their mutual relations.

Cybersecurity is also a necessary element of the proper development of society in terms of organizing and managing state defense, both in the context of national security at virtually every level of society and administration[2].

The concept of cybersecurity is identified with the security of information systems, combining this concept with IT security. This approach draws on the provisions of ISO/IEC 727032, which defines cybersecurity as maintaining confidentiality, availability, and integrity, although it is noted that it is also possible to include other security properties, such as authenticity, accountability, non-repudiation, and reliability in cyberspace[3].

The definition of cybersecurity proposed by the National Initiative for Cybersecurity and Studies, which is an organization managed by the Cybersecurity and Communications Education and Awareness Division of the US Federal Government, is defined as a situation ensuring that information or communication systems and the information contained therein are secured, protected against damage, unauthorized use, modification or exploitation[4].

And what did the development of cybersecurity look like at NATO summits?

Historically, the 2002 Prague Summit first marked NATO's tasking authority committee with regards to all activities that should be held in relations to

1 E. Hodyr, *Cybersecurity – new challenges in international law*, „Journal of Polish American – Science and Technology" 2016, vol. 10.
2 *Leksykon cyberbezpieczeństwa*, red. K. Chałubińska-Jentkiewicz, Warszawa 2024, s. 63.
3 *Strategia cyberbezpieczeństwa RP na lata 2019–2024*, Warszawa 2019.
4 Z. Chmielewski, *Polityka publiczna w zakresie ochrony cyberprzestrzeni w UE i państwach członkowskich*, „Studia z Polityki Publicznej" 2016, no. 2, s. 108.

Cyber-Defence. As technical achievements were delivered, so did policy-makers, deliver policy results on Cyber-defence.

That is why, Allied leaders during the Riga Summit of 2006 acknowledged the need to include as is stated on its decisions at the Press Communique: 1) protect NATO's operational information systems, 2) protect its allied countries from any e-, or in other words cyber-attacks by new forms and means developed by NATO's Allied Command Transformation (ACT)[5]. In turn, the October 2007 outcomes of NATO, at the level of Allied Defence Ministers, gave way to the inauguration of NATO's centre of excellence (COE) by the Allied Command Transformation on Cyber-Defence, in Estonia–Tallinn. It is based, on the aforementioned Concept on Cyber-Defence, as agreed by NATO's Military Committee[6].

At the 2008 Romanian Summit, the Head of State and Government drafted the first cyber policy. At the 2010 Lisbon Summit, the Cyber Defense Concept was adopted. At the important 2016 Warsaw Summit, cyberspace became the next domain of warfare. At the 2019 London Summit, Jens Stoltenberg declared NATO's readiness. At the 2023 Vilnius Summit, cybersecurity-related activities were tested in practice. For example, soldiers from the Cyberspace Defense Forces ensured the security of the summit as part of an allied initiative.

In 2022, at the NATO Summit in Madrid, Allies decided to create and develop capabilities to rapidly respond to malicious cyber activities. These capabilities were first tested during the NATO Summit in Vilnius. Allies launched and tested the new capabilities as part of the Virtual Cyber Incident Support Capability (VCISC) initiative. During the NATO Summit in Vilnius, Allies from Lithuania, Poland, Belgium, the Netherlands, Turkey, Slovakia, Slovenia, Spain, Norway, Estonia, and Albania tested communication and coordination procedures. Leading NATO cybersecurity experts connected remotely to the Lithuanian network to provide additional technical support to the Lithuanian National Cyber Security Centre.

5 M.P. Efthymiopoulos, *Challenging NATO's Security Operations in Electronic Warfare: the Policy of Cyber-Defence: the Case of Greece; Nato's Concept of Cyber-Defence*, https://www.lse.ac.uk/Hellenic-Observatory/Assets/Documents/HO-PhD-Symposia/The-4th-HO-Phd-Symposium/25-June/Session-3/Panel-2-Foreign-Security-Policy.pdf [access: 17.01.2026].

6 Ibidem.

VCISC is a cyber support service provided by Allies to other Allies on a voluntary basis. Allied support may also include nationally designated trusted industry partners. VCISC support provided by Allies is part of NATO's overall deterrence and defense posture[7]. Next I would like describe organization related with cybersecurity.

NATO structures serve, above all, as support to the decision-making process. For that purpose, the North Atlantic Council is supported by the Cyber Defence Committee, responsible for the political governance of NATO's cyber defence. The Cyber Defence Management Board (CDMB) within the Emerging Security Challenges Division, gathers in a permanent coordination format the representatives of the military, diplomatic and technical bodies (commands, agencies, etc.), responsible for the various NATO cyber defence activities.

At the operational level, in 2019 a Cyberspace Operations Centre (CYOC) was created within the Allied Command Operations (ACO) in Mons, Belgium. The Centre is responsible for NATO cyber operations, in support of operational commands primarily for monitoring cyberspace and coordinating operations in this domain with those in the land, maritime and air domains. The CYOC could pave the way to the future creation of a NATO command for cyber operations on par with operational commands in the other domains. Beyond the CYOC and its possible evolution, almost all the main elements of NATO integrated military command already have a role to play with regard to cyber defense. As an example, the NATO Force Integration Units (NFIUs) are deployed in the Eastern flank countries to better integrate local forces, from the Baltic to Romania, with those of other member states in order to ensure deterrence and defense vis-à-vis Russia.

At the technical level, the NATO Communications and Information Agency (NCIA), established in 2012, provides many of the capabilities necessary to the Alliance's structures in terms of cyber defense. Moreover, the NCIA directly manages some of the allied networks, interacting with the NATO Cyber Security Centre (NCSC) and the NATO Computer Incident Response Capability (NCIRC). The latter constantly monitors the Alliance's

7 *DKWOC na szczycie NATO w Wilnie*, https://www.wojsko-polskie.pl/woc/articles/aktualnosci-w/dkwoc-na-szczycie-nato-w-wilnie/ [access: 17.01.2026].

networks, is the first to respond in the event of attacks, files reports on similar instances and provides support to the aforementioned CDMB. Furthermore, the NCIRC, through a specific coordination center, allows Allies to exchange information and techniques on cyber threats, including some indicators that can provide clues over the nature of occurred attacks.

Outside the Allied integrated military command, the Cooperative Cyber Defence Centre of Excellence (CCDCOE), inaugurated in Estonia in 2008, prepares studies and reports on issues of interest for cyber defence and, since 2010, hosts periodic exercises. One of such exercises, known as Locked Shield, involved more than one thousand participants in 2019, including institutional leaders and personnel devoted to responding to cyber-attacks, virtually engaged in containing a series of attacks to the critical infrastructures of a country during political elections. Such exercises are very important to prepare civil and military personnel for worst-case cyber-attack scenarios. However, the training should also touch upon people's habits in using electronic devices that weaken NATO's defense capability. The human factor is crucial for cyber defense. In this context, a contribution to allied defense capabilities and resilience is provided by the training courses of the NATO Communications and Information Systems School(NCISS) in Portugal and the NATO school in Oberammergau, Germany, as well as by the research activities on the politico-military level of the NATO Defence College in Rome[8].

These organizations are primarily for training or defense purposes. To maintain security within the alliance, I believe that cooperation with the private sector is also necessary to help protect infrastructure. in 2014 the Alliance launched the NATO Industry Cyber Partnership (NICP)[9], which envisages, among other things, the participation of industrial representatives in the annual Cyber Defence Workshop, aimed at exchanging highly technical information on threats, vulnerabilities and possible solutions among Allies. The industrial partners, moreover, frequently report to competent NATO structures on the evolution and trends observed in the cyber domain, including the security challenges associated with specific technologies, thus contributing

8 *Cyber Defence in NATO Countries: Comparing Models*, https://www.iai.it/it/pubblicazioni/c03/cyber-defence-nato-countries-comparing-models [access: 17.01.2026].

9 *NATO Industry Cyber Partnership*, https://www.ncia.nato.int/business/partnerships/nato-industry-cyber-partnership.html [access: 17.01.2026].

to the allied reflection on this topic[10]. I will discuss EU cybersecurity later. For now, I think it's worth mentioning the cybersecurity of Polish diplomatic missions.

Russia's full-scale aggression against Ukraine began on February 24, 2022, with the entry of Russian military forces into Ukrainian territory. However, the confrontation in cyberspace has been ongoing since at least 2014, i.e., the illegal annexation of Crimea and eastern Ukraine. Russian hackers aim to disrupt Ukrainian military, civilian, and government networks and disrupt communications, primarily through destructive attacks on systems and databases. In addition to these types of activities, Russians also use hacking operations to obtain information to support the war effort (cyberespionage).

One of the conditions for ensuring the stability of the North Atlantic Alliance, its member states, and the citizens of the Western community is the neutralization of the threat posed by hostile operations conducted in cyberspace[11].

The document was adopted in July 2016 during the NATO summit in Warsaw. Cyberspace was then recognized as the next – fifth – operational domain (alongside land, sea, air, and space).

In peacetime, NATO allies focus on deterring and repelling attacks in cyberspace. There are numerous initiatives supporting these activities, such as the „EU Cyber Diplomacy Toolbox", a set of tools for diplomacy in cyberspace. This initiative was created as a joint EU diplomatic response to malicious activities in cyberspace, including numerous hacker attacks[12].

All diplomatic efforts promote security and stability in cyberspace by strengthening international cooperation and reduce the risk of misperceptions, escalations, and conflicts that may result from ICT incidents[13].

Russian actions are hostile not only to Ukraine, but also to Poland and the West. Malicious cyber activities targeting allied countries include, among

10 *Cyber Defence in NATO Countries...*

11 *Analiza zagrożeń dla cyberbezpieczeństwa placówek dyplomatycznych RP oraz innych państw NATO w kontekście wybranych ataków hakerskich*, https://www.gov.pl/web/baza-wiedzy/analiza-zagrozen-dla-cyberbezpieczenstwa-placowek-dyplomatycznych-nato [access: 17.01.2026].

12 Ibidem.

13 *The Cyber Diplomacy Toolbox*, https://www.cyber-diplomacy-toolbox.com/ [access: 18.01.2025].

others, the theft of sensitive information (gaining unauthorized access to protected network resources), operations using encryption software (ransomware), destructive software (wiper), and distributed denial of service (DDoS) attacks[14].

Further, it should be noted that in 2016, NATO recognized cyberwarfare as another operational domain, and hybrid and cyberattacks may constitute grounds for collective defense under Art. 5 of the North Atlantic Treaty. For less serious acts, allies also have Art. 4 of the Treaty, which allows for consultations whenever one of them believes that the „territorial integrity, political independence, or security" of an ally is threatened.

As a side note, NATO countries must focus on strengthening their cyber resilience and defense capabilities. Their efforts include investing in cybersecurity, developing capabilities to detect and respond to attacks, strengthening critical infrastructure, and international cooperation to share information and jointly address cyber threats.

Diplomatic missions are also at risk due to the war in Ukraine; many of them are involved in obtaining aid funds and coordinating their transport to Ukraine. Analysts from the Polish Intelligence Agency, working with entities within the National Cybersecurity System, are observing numerous attempted attacks on Polish diplomatic missions. One of the most active and, at the same time, most dangerous organizations attempting to breach their security is a group known as APT29 (also known as NOBELIUM, The Dukes, Cozy Bear, BlueBravo). It is linked to the Foreign Intelligence Service of the Russian Federation (as established by the governments of the United States and Great Britain, among others). APT29's connections with Russian intelligence indicate that its activities are directed against NATO countries – in line with generally accepted Russian practices. The APT29 group's operations largely begin with mass emails designed to encourage embassy employees to open an attachment or hyperlink leading to a fake website. Cyberattacks also took the form of fake invitations to receptions, diplomatic meetings, and offers to sell various goods with discounts for diplomats.

Besides Russia, China is another source of threat to Western IT networks. Besides the struggle for influence, China seeks to eliminate the scientific and

14 An attack that disrupts the availability of a service by overloading it.

technological advantages of Western countries in many fields, particularly in industry and modern technologies. Chinese hacker groups include APT27, APT30, APT31, Ke3chang, Gallium, and Mustang, Panda. Mustang Panda (also known as EarthPreta, BronzePresident, CamaroDragon) is a hacking group that has been operating since at least 2017. It primarily engages in data theft and spying on states and private sector companies. It uses advanced tools and techniques such as spearphishing or exploits software vulnerabilities. Its targets primarily include the energy, industrial, and defense sectors. The group is considered one of the most active and technologically advanced in China.

Poland will likely remain a target of attacks by groups sponsored by foreign governments, particularly Russia. These attacks are a symptom of hybrid activities against countries supporting Ukraine, among which Poland plays a special role. The activity of these organizations may be particularly dangerous given the upcoming parliamentary elections in Poland (autumn 2023). The introduction of the Charlie CRP alert level and its maintenance since February 2022 was a response to the growing scale of hacker attacks and allowed for a more efficient response to threats in cyberspace.

The Ministry of Digital Affairs conducts numerous activities to counteract threats to Poland's cybersecurity, including: The Cybersecurity Cooperation Program (PWCyber) – a collaboration between the public and private sectors. Over 30 companies from the technology sector participate, with more joining gradually. It organizes training courses, workshops, and knowledge exchange; preparing periodic studies on cyber threats and organizing training on: coordinating activities at the national level, including by providing tools for secure overt and classified communications, including organizing periodic meetings on the state of security; participating in numerous international initiatives on cybersecurity, such as the Counter Ransomware Initiative[15].

Moving on, we can ask ourselves what NATO's cybersecurity goals are. There are: Cyber crime, Cyber espionage, Cyber terrorism, Cyber warefare.

Further analyzing NATO's cybersecurity, NATO's first priority has always been to defend the North Atlantic area, and, even though cyber threats emanate from cyberspace, the alliance's doctrine is still, for the most part, focused on the protection of its own computer networks.

15 *Analiza zagrożeń dla cyberbezpieczeństwa placówek dyplomatycznych…*

Second, NATO's cyber security doctrine and posture is still largely defensive. The alliance has not been involved in developing offensive cyber attack capabilities. Third, although deterring cyber attacks is clearly not as straight forward as deterring conventional attacks from state actors, NATO cyber doctrine appears to be based in deterrence by denial. Fourth, NATO's cyber security posture is now based primarily on states and state-sponsored hackers. Lastly, as with many other areas of NATO's security doctrine, NATO's approach to cyber security is based around developing cooperative relationships, both internally and externally.

The institutional development of NATO's cyber security role. 1999 Cyber attacks directed against NATO during the Kosovo conflict 2002 Prague summit – Cyber security appears on NATO's formal agenda for the first time. Computer Incident Response Capability (NCIRC) formed. Cyber Defence Programme established 2006 Riga Summit – Emphasis placed on the security of NATO's own information systems 2007 Cyber attacks against Estonia focus attention within NATO on the strategic issues involved 2008 NATO Cyber Defence Policy approved by the NAC, Cyber Defence Management Authority (CDMA) created, NATO Cooperative Cyber Defence Centre of Excellence (CCD COE) established 2010 Cyber Security appears in NATO's 2010 Strategic Concept and forms one of the pillars of the NATO Emerging Security Challenges Division 2011 Revised Policy on Cyber Defence Adopted – emphasis on defence rather than deterrence, 2012 Rapid Reaction Team (RRT) becomes operational, 2013 Tallinn Manual on the International Law Applicable to Cyber Warfare released, 2014 NATO adopts an enhanced Cyber Defence Policy through which cyber attacks become part of NATO's Art. 5 outlook[16].

Moving on, I'd like to describe European organizations, offices, and positions related to cybersecurity. First, the EU Cyber Diplomacy Toolbox. What is cyber diplomacy? Cyber diplomacy is the conduct of foreign policy, negotiation, and international coordination on matters that substantially affect activity in and through digital networks. It is the application of diplomatic method and legal reasoning to a domain in which the objects of negotiation can be packets, protocols, software supply chains, cryptographic keys, and

16 J. Burton, *NATO's cyber defence: Strategic challenges and institutional adaptation*, „Defence Studies" 2015, no. 4, p. 13.

data. The aim remains diplomatic in shaping expectations, forging consent, and preventing conflict.

Cyber diplomacy, emerging risks and challenges

Cyber diplomacy has moved into a domain where technological acceleration, strategic competition, and legal fragmentation interact in complex and often destabilizing ways. A new generation of risk alters state responsibility, liability, attribution, sanctions exposure, market access, insurance coverage, procurement integrity, and the enforceability of cross-border obligations.

The widening gap between technical capability and legal containment**.** The core diplomatic risk in cyberspace is that capability is scaling faster than law can contain it. Machine learning models and automated tools have lowered the cost of targeted intrusion, information operations, and deception, enabling a level of persistence and precision previously reserved for a few intelligence services.

AI-enabled deception, reputational coercion, and negotiation manipulation. Generative systems have turned social media and information space into an operational battlespace. For cyber diplomacy, there are three new risks:

1) impersonation of diplomatic principals and institutions, where deepfake voice and video are used to manipulate policy concessions, spread confusion during crises, or discredit international organizations. This includes market manipulation, fraudulent instructions, and the triggering of actions;
2) targeted cognitive pressure on individual negotiators, where behavioral data are mined to craft manipulative engagement;
3) the contamination of evidentiary chains, where fabricated or subtly altered digital documents appear in investigative or dispute resolution records.

Space-cyber convergence**.** The integration of space and cyber systems has created new points of coercion. Commercial satellite constellations, navigation services, and ground segment operations have become critical infrastructure.

Mercenary cyber capability markets and the privatization of coercion**.** An increasingly sophisticated market of surveillance tools, exploit brokers, and

offensive security contractors operates across jurisdictions. From a diplomatic perspective, the risk is deniable coercion deployed by private actors with plausible distance to states, enabling influence operations, transnational repression, or targeted intrusions that would be diplomatically costly if conducted by official services.

The privatization of coercion occurs when those services are used to exert political, economic, or legal pressure by states, corporations, criminal groups, or shadow intermediaries, so that the coercive act can not be directly associated with the principal who benefits. In very simple words, instead of a government ordering a clandestine operation, a government, or state-sponsored entity hires a private operator to do the dirty work, creating plausible deniability, reducing the political cost, and increasing the scale and availability of offensive capability. The Paris Call for Trust and Security in Cyberspace.

The Paris Call for Trust and Security in Cyberspace, launched on 12 November 2018 during the Paris Peace Forum, deals with emerging and insufficiently regulated cyber challenges. States, businesses (including Microsoft, Kaspersky, Siemens, Google, Facebook), professional associations and civil society organizations discuss to find solutions for the regulation in cyberspace, the practicability of international law, and the responsible behaviour of States. 11.11.2021 – The European Union and the United States have joined the Paris Call. Their decision will strengthen the Call and enable it to go further in the defence of stability in cyberspace.

The 9 principles – The Paris Call for Trust and Security in Cyberspace:

1) protect individuals and infrastructure;
2) protect the Internet;
3) defend electoral processes;
4) defend intellectual property;
5) non-proliferation;
6) lifecycle security;
7) cyber hygiene security;
8) no private hack back;
9)international norms[17].

17 *What is cyber diplomacy?*, https://www.cyber-diplomacy-toolbox.com/Cyber_Diplomacy.html [access: 17.01.2026].

The EU's main cybersecurity organization is ENISA (European Union Agency for Cybersecurity), which handles policy, certification, and capacity building, supported by bodies like the European Cybersecurity Competence Centre (ECCC) for industrial capacity, the European Cyber Security Organisation (ECSO) (public-private), and CERT-EU for EU institutions, all working under the broader EU Cybersecurity Strategy to boost resilience and response to cyber threats.

Key EU Cybersecurity Organizations:

- European Union Agency for Cybersecurity (ENISA) – the central agency for EU cybersecurity, responsible for policy advice, developing certification schemes (like for ICT products), sharing knowledge, and enhancing Europe's cyber resilience;
- European Cybersecurity Competence Centre (ECCC) – aims to boost Europe's cybersecurity industry and technological capabilities, working with national centers;
- European Cyber Security Organisation (ECSO) – a non-profit, private-public partnership that develops Europe's cybersecurity resilience and strategic autonomy.
- Computer Emergency Response Team for the EU (CERT-EU) – focuses on cybersecurity for EU institutions, bodies, and agencies.

Key Initiatives & Frameworks:

- EU Cybersecurity Act: Strengthens ENISA's role and established the EU-wide cybersecurity certification framework;
- EU Cybersecurity Strategy – A broad plan for internal market security, law enforcement, diplomacy, and defense, including collective response to major attacks;
- EU Cyber Diplomacy Toolbox – A framework for diplomatic restrictive measures against malicious cyber activities;
- EU CyCLONe – A network for coordinating responses to large-scale cyber incidents, supported by ENISA[18].

18 *AI review*, https://www.google.com/search?q=EU+organization+cybersecurity&oq=EU+organization+cybersecurity&gs_lcrp=EgZjaHJvbWUyBggAEEUYOTIICAEQABgWGB4yBwgCEAAY7wUyBwgDEAAY7wUyBwgEEAAY7wUyBwgFEAAY7wUyCggGEAAYgAQYogTSAQoxNzM4NGowajE1qAIIsAIB8QVLaFXkDNCZew&sourceid=chrome&ie=UTF-8 [access: 17.04.2026].

European Commission:

- Directorate-General for Digital Services (DIGIT): Leads the Commission's digital transformation, ensuring the digital landscape is robust, resilient, and secure. DIGIT also leads the CERT-EU, a cybersecurity service for EU institutions, bodies, offices, and agencies;
- Directorate-General for Communications Networks, Content and Technology (DG Connect): Works to strengthen Europe's digital future and cybersecurity by funding and regulating digital technologies. It enforces rules for digital platforms, markets, and AI, helps defend against cyber threats, and promotes digital skills.

Other EU Institutions:

- European Parliament's DG ITEC: Develops and maintains secure and resilient ICT services for the Parliament;
- Council of the European Union's DITEC: The Directorate-General for Digitalisation, Information Technology and Cybersecurity (DITEC) is responsible for the Council's cybersecurity governance, policy, and incident response.

Key Aspects of EU Cybersecurity:

- Regulation: The EU has established a Cybersecurity Regulation to ensure a high common level of cybersecurity across all its institutions, bodies, offices, and agencies;
- Certification: The EU Cybersecurity Act gives ENISA (the European Union Agency for Cybersecurity) the mandate to set up and maintain a European cybersecurity certification framework;
- Strategy: The EU's Cybersecurity Strategy aims to increase resilience, build response capacities, and foster international cooperation;
- Partnerships: The EU works with partners to strengthen its digital leadership, promote global standards, and counter disinformation.

I've described cybersecurity in NATO and the EU above. I believe it's important for both organizations to cooperate, which I'll describe below. The formal establishment of relations between NATO and the European Union can be considered the exchange of letters in January 2001 between NATO

Secretary General Lord George Robertson and Swedish Foreign Minister Anna Lindh, then serving as President of the Council of the European Union[19].

Despite its rather general format, this exchange of letters was the first formal agreement on consultation and cooperation between NATO and the European Union. Previously, joint meetings of the bodies of both organizations had taken place, including the interim Political and Security Committee and the North Atlantic Council, but since the exchange of letters, these have become regular[20]. Further cooperation between NATO and the EU was defined by the EU Declaration on European Security and Defence Policy (ESDP) of 2002. In March 2003, the Berlin Plus concept was signed.

The Berlin Plus package of agreements initially included several components, including:

- guaranteeing the EU access to NATO planning capabilities;
- the assumption that the EU would gain access to pre-defined NATO assets and capabilities for its operations;
- defining European command options for EU operations within NATO's integrated command structure, including clarifying the responsibilities of the Deputy Supreme Allied Commander Europe in the context of cooperation with the EU;
- further adapting the NATO defence planning system to take into account the greater availability of forces for EU operations[21].

Key points of NATO-EU cybersecurity cooperation:

- strategic partnership
- joint action against hybrid threats
- building capabilities and resilience
- increased information sharing.

Crisis Management and Incident Response: Coordination of cyber crisis management mechanisms and a common approach to preventing, deterring,

19 The formal establishment of relations between NATO and the European Union can be considered the exchange of letters in January 2001 between NATO Secretary General Lord George Robertson and Swedish Foreign Minister Anna Lindh, then serving as President of the Council of the European Union.

20 J. Zajączkowski, *Unia Europejska w stosunkach międzynarodowych. Wymiar polityczny*, Warszawa 2006, p. 243, 251–252.

21 A. Bugajski, *Problemy i wyzwania w stosunkach NATO – Unia Europejska*, Warszawa 2023, p. 109, 113.

and responding to malicious cyber activities. Exercises and Training: Observation and mutual participation in cyber defense exercises (e.g., the annual NATO „Cyber Coalition" exercise) to enhance crisis preparedness and mutual understanding of tools and practices[22].

Conclusion

Currently, the way conflicts and wars are being fought is changing. Cyberattacks are the first to occur. They are becoming increasingly common in Poland and Western countries. For this reason, we must be ready to prevent and defend against them. Cooperation between NATO and the EU is crucial. It's also crucial to collaborate with the private sector, which will help defend infrastructure. I believe that NATO and EU cooperation is crucial in a changing world. This is also possible during the Europeanization of NATO.

Bibliography

Analiza zagrożeń dla cyberbezpieczeństwa placówek dyplomatycznych RP oraz innych państw NATO w kontekście wybranych ataków hakerskich, https://www.gov.pl/web/baza-wiedzy/analiza-zagrozen-dla-cyberbezpieczenstwa-placowek-dyplomatycznych-nato [access: 17.01.2026].

Bugajski A., *Problemy i wyzwania w stosunkach NATO – Unia Europejska*, Warszawa 2023.

Burton J., *NATO's cyber defence: Strategic challenges and institutional adaptation*, „Defence Studies" 2015, no. 4.

Chmielewski Z., *Polityka publiczna w zakresie ochrony cyberprzestrzeni w UE i państwach członkowskich*, „Studia z Polityki Publicznej" 2016, no. 2.

Cyber Defence in NATO Countries: Comparing Models, https://www.iai.it/it/pubblicazioni/c03/cyber-defence-nato-countries-comparing-models [access: 17.01.2026].

DKWOC na szczycie NATO w Wilnie, https://www.wojsko-polskie.pl/woc/articles/aktualnosci-w/dkwoc-na-szczycie-nato-w-wilnie/ [access: 17.01.2026].

Efthymiopoulos M.P., *Challenging NATO's Security Operations in Electronic Warfare: the Policy of Cyber-Defence: the Case of Greece; Nato's Concept of Cyber-Defence*, https://www.lse.ac.uk/Hellenic-Observatory/Assets/Documents/

HO-PhD-Symposia/The-4th-HO-Phd-Symposium/25-June/Session-3/Panel-2-Foreign-Security-Policy.pdf [access: 17.01.2026].
Hodyr E., *Cybersecurity – new challenges in international law*, „Journal of Polish American – Science and Technology" 2016, vol. 10.
Leksykon cyberbezpieczeństwa, red. K. Chałubińska-Jentkiewicz, Warszawa 2024.
NATO Industry Cyber Partnership, https://www.ncia.nato.int/business/partnerships/nato-industry-cyber-partnership.html [access: 17.01.2026].
Strategia cyberbezpieczeństwa RP na lata 2019–2024, Warszawa 2019.
The Cyber Diplomacy Toolbox, https://www.cyber-diplomacy-toolbox.com/ [access: 18.01.2025].
What is cyber diplomacy?, https://www.cyber-diplomacy-toolbox.com/Cyber_Diplomacy.html [access: 17.01.2026].
Zajączkowski J., *Unia Europejska w stosunkach międzynarodowych. Wymiar polityczny*, Warszawa 2006.

Cyberbezpieczeństwo w NATO i Unii Europejskiej

Streszczenie

Celem artykułu jest zebranie i uporządkowanie wiedzy na temat cyberbezpieczeństwa, a także identyfikacja i analiza strategicznych wyzwań w obszarze cyberbezpieczeństwa, stojących przed NATO i Unią Europejską. Autorka omawia zagadnienia cyberbezpieczeństwa misji dyplomatycznych w kontekście wojny w Ukrainie.

Słowa kluczowe

cyberbezpieczeństwo, NATO, Unia Europejska, strategia, misja dyplomatyczna, współpraca