Nicoleta Annemarie MUNTEANU
Lucian Blaga University of Sibiu, Romania

NATO'S MECHANISMS FOR THE GOVERNANCE OF CYBERSECURITY

Abstract:	*In the current context of escalating digital threats, cybersecurity has emerged as a critical pillar of NATO's collective defense framework. The Alliance formally recognizes cyberspace as an operational domain, alongside land, air, maritime, and space, signifying that a major cyberattack may trigger Article 5 of the Washington Treaty, which pertains to collective defense.* *NATO collaborates closely with its member states to enhance cyber resilience by facilitating real-time information sharing, conducting joint exercises, and supporting the development of advanced national capabilities. The Cooperative Cyber Defense Centre of Excellence in Tallinn, Estonia, plays a pivotal role in training specialists and testing defensive strategies.* *Cyber threats often emanate from both state and non-state actors and are characterized by attacks on critical infrastructure, data theft, disinformation campaigns, and attempts to undermine democratic institutions. NATO addresses these multifaceted challenges through a cooperative international approach, fostering partnerships, including private sector, and by integrating emerging technologies such as artificial intelligence and advanced data analytics.* *Consequently, cybersecurity transcends the military sphere, constituting a shared responsibility that engages all segments of society. Through coordinated actions and proactive strategies, NATO reinforces its role as a guarantor of peace and security in the digital age.*
Keywords:	**NATO; cyber security; cyber defense; CCDCOE; Estonia; strategic concepts; Article 5**
Contact details of the authors:	**E-mail:** nicoleta.munteanu@ulbsibiu.ro
Institutional affiliation of the authors:	**Lucian Blaga University of Sibiu, Department of International Relations, Political Sciences and Security Studies**
Institutions address:	550324-Sibiu, Calea Dumbrăvii nr. 34, Tel./ Fax: 0040/269/422169

Introduction

Even though NATO has always protected its information systems and communication, an important moment in time being the cyber-attacks against Estonia's public and private institutions in 2007, our purpose is not to present a detailed chronology of the NATO history in this context, but only the most important recent approaches. Iti is worth mentioning that because of these events, the Allied Defense Ministers approved of their first Policy on Cyber Defense in January 2008[1]. Starting with 2010 the North-Atlantic Alliance Organization Strategic Concept proposed a new approach related to the need of adapting to the new security threats environment, to manage the increasing context of cybersecurity, terrorism, transit routes for energy and trade, global climate change, technology[2]. The 2021 NATO Summit in Brussels proposed the Comprehensive Cyber Defense Policy[3], a document

[1]North Atlantic Treaty Organization, *Cyber Defense*, https://www.act.nato.int/activities/cyber/ (12.04.2025)
[2] Albulena Halili, *Non-traditional Security Threats and NATO`s Response in the Contemporary Security Environment*, "SEEU Review", Vol. 18, No. 2, 2023, DOI: 10.2478/seeur-2023-0095, p. 149

supporting NATO`s purposes in terms of its overall defense posture and deterrence. Another important moment is the 2022 Madrid NATO Summit which reevaluated the cyberspace as a complex and contested arena, in terms of cyberoperations, cyberattacks, cyberweapons, cyberspace, cyber enabled disinformation[1]. NATO continued to achieve new strategies to manage the cyber defense at the 2023 NATO Summit in Vilnius and integrated Nato`s cyber defense levels as technical, military, and political, in terms of civil-military cooperation, also engaging the private sector[2].

At the 2024 NATO Summit in Washington, D.C., the Allies agreed to establish the NATO Integrated Cyber Defense Centre to enhance network protection, situational awareness and the implementation of cyberspace as an operational domain. The most important institutions which are involved in this area are: the NATO Integrated Cyber Defense Center (NICC) in Mons, Belgium, established in July 2024; the NATO Cooperative Defense Centre of Excellence (CCDCOE) in Tallin, Estonia[3] established in 2008. CCDCOE hosted in May 2025 the Locked Shields 2025 cyber defense exercise, gathering almost 4000 experts representing 41 NATO ally and partner nations[4]. All the trainings and exercises are conducted by CCDCOE, within the Crossed Swords annual technical red teaming cyber exercise training penetration tester, digital forensic experts and situational awareness exerts[5]; The NATO Communications and Information (NCI) Academy in Oeiras, Portugal (2029)[6]; The NATO School in Oberammergau, Germany; The NATO Defense College in Rome, Italy (1951)[7]. Even though this concern could be considered as a new one, it is important to mention that the first cyber crisis happened in Kosovo air campaign in 1999, when NATO`s e-mail accounts were blocked, and the website was disrupted[8]. In that period, cyber dimensions of a conflict used to be considered as subordinating to conventional warfare. Some authors consider that although threats of cyber-attacks are or the first time mentioned verbatim in the 2002 Prague Summit Declaration, the year of 1999 is the one which could be seen as the key milestone, as the first recognition and jumpstart of NATO`s perspective on cyber defense. The research mentioned before presents as two important events - the cyber-attacks orchestrated by Serbian and Russian hackers against NATO networks and systems during the Kosovo War and the mistaken bombing of the Chinese embassy in Belgrade[9].

In this context, we consider worthy to mention NATO Strategic Communication (STRATCOM) as an important aspect of consolidated action related to all the hybrid threats area[10]. Given the paramount importance and inherent complexity of cybersecurity in the contemporary world, it is evident that organizations such as NATO play a critical role in addressing these multifaceted challenges. The digitalization of conflicts and crises is becoming increasingly tangible in the present era. Traditional instruments of warfare - aircraft, bombs, and missiles - are progressively being supplanted by cyberattacks, malware, and disinformation campaigns. In the digital realm, adversaries can test security frameworks with a mere click of a mouse. Consequently, global criminal cyberattacks, the aggressive exploitation of social media by groups such as Daesh to incite terrorism, and the alleged role of

---

[3] North Atlantic Treaty Organization, *Cyber Defense*, 30th of July 2024, https://www.nato.int/cps/en/natohq/topics_78170.htm#:~:text=At%20the%202021%20NATO%20Summit%20in%20Brussels%2C%20Allies,well%20as%20its%20overall%20deterrence%20and%20defence%20posture (16.05.2025)

[1] Research Division NATO Defence College Rome, *Strategic Shifts and NATO`s New Strategic Concept,* NATO Defense College, Rome, 2022, pp. 32-36

[2] *Idem*

[3] NATO Cooperative Cyber Defence Centre of Excellence, https://ccdcoe.org/about-us/ (17.04.2025)

[4] Eduard Kovacs, *41 Countries Taking Part in NATO`s Locked Shields 2025 Cyber Defense Exercise,*"Security Week", May 7, 2025, 41 Countries Taking Part in NATO's Locked Shields 2025 Cyber Defense Exercise - SecurityWeek (12.05.2025)

[5] Marko Arik, *How Do NATO Members Define Cyber Operations?,* "Communications in Computer and Information Science", December 2023, DOI: 10.1007/978-3-031-49212-9_2, pp. 8-14

[6]NATO Communications and Information (NCI) Academy in Oeiras, Portugal, NATO Communication and Information - Academy | QA Hub - NATO QA Programme (21.04.2025)

[7] North Atlantic Treaty Organization, *Cyber Defense*, 30th of July 2024, https://www.nato.int/cps/en/natohq/topics_78170.htm#:~:text=At%20the%202021%20NATO%20Summit%20in%20Brussels%2C%20Allies,well%20as%20its%20overall%20deterrence%20and%20defence%20posture (16.05.2025)

[8] Bildiri Kitabi, *On the Individual, Society, and Politics in a Digitalized World*, Ivik University, Istanbul, 2022, p. 157

[9] *Idem*

[10] Igor Gjoreski, Zoran Nacev, *Global Security Trends in Euro-Atlantic Area and NATO New Strategic Concept,* "Security Dialogues", Vol. 13, No.2, 2022, DOI: 10.47054/SD22132023gj, p. 62

Russia in disseminating disinformation and fomenting confusion exemplify the evolving threat landscape confronting NATO. This underscores the Alliance's exposure to a complex and rapidly shifting threat environment. Cyberattacks may be perpetrated by both state and non-state actors during military operations. Hybrid warfare has also encompassed cyber intrusions, information leaks, and espionage in recent events. Cyber incidents bear geopolitical ramifications and can jeopardize the security, stability, and economic well-being of the Alliance as a whole. NATO currently faces a formidable challenge: how to safeguard itself and its member states against the pernicious power wielded in cyberspace.

The Approach to Cybersecurity at NATO Level

The evolution of NATO's cybersecurity domain has been driven by heightened awareness and the progressive strengthening of incident response capabilities. Positioned at the forefront of cyber defence, NATO has successfully enhanced its cyber capabilities through comprehensive training, education, and rigorous exercises. The 2021 Comprehensive Cyber Defence Policy builds upon NATO's core missions as well as its overarching defence posture and deterrence, thereby enabling the Alliance to further bolster its resilience. Continuously advancing its cybersecurity defence framework, NATO has demonstrated a remarkable capacity to adapt and respond to emerging challenges in the cyber defence landscape through collaboration, information sharing, and sustained training initiatives[1]. Experts from the CCDCOE consider that the weaponization of the internet represents one of the most dangerous trends of development of modern cyberspace, and the modern military structures are ready to use it as a parallel battlefield[2], knowing that space and time considerable changes in the last decades, one of the reasons being the exponential increase of technology.

Among the firsts steps of NATO`s approaches were to establish a theoretical framework for the cyber terminology accepted by the member states, as a common understanding, an important aspect directly related to the interoperability necessary within the NATO activity in this area. CCDCOE mentioned before had an important role, also the information from the governmental sources and military field, as it is presented in Figure 1.

	Data sources		
	GOV	MIL	CCDCOE
CAN	6	-	-
EE	5	-	-
FRA	5	-	-
GER	1	1	1
ITA	6	-	1
LIT	3	-	1
NL	6	-	-
ES	5	-	1
SWE	1	1	-
TUR	2	-	1
UK	4	-	-
USA	8	2	-

Figure 1. Data sources of NATO Cyber Operations Doctrinal Publications[3]

[1]NATO, *Cyber Defense,* https://www.nato.int/cps/en/natohq/topics78170.htm (27.03.2025)

[2] Christian Czosseck, Kenneth Geers (Eds.), *The Virtual Battlefield: Perspectives on Cyber Warfare,* IOS Press, Amsterdam, Berlin, Tokyo, Wahington, DC, 2009, pp. 119-121

[3] Marko Arik, *How Do NATO Members Define Cyber Operations?,* "Communications in Computer and Information Science", December 2023, DOI: 10.1007/978-3-031-49212-9_2, p. 4

The NATO members states have a comparable understanding of the cyber-related terminology, also similar organizational and logistic infrastructure, as a part of their commitment to realizing and respecting the NATO strategic purposes. In 2021 CCDCOE provided a comparative study on the cyber defense of Alliance`s members states, focused on terminology mostly[1]. This study clarified the confusion between the terms cyber defense and cyber security, considering that there is no uniform distinction between them[2], adding though that could be ne noticed a certain distinction whether is used in a civilian or military environment[3]. Since 2016 a series of publications on cybersecurity and its terminology have been released by NATO Joint Publications, that contributed to the establishing of t mutual approach in terms of the theoretical framework for the member states. Within the doctrinal publications of the study mentioned before selected countries, there were indicators of the distribution of the publications and whether cyberoperations are defined, as it is presented in Figure 2. It is important to mention in this context of 2016 that at the Warsaw Summit, for the first time NATO declared cyberspace as a military domain, and one year later the Secretary General Jens Stoltenberg delivered the NATO Cyber Operations Center (CYOC)[4].

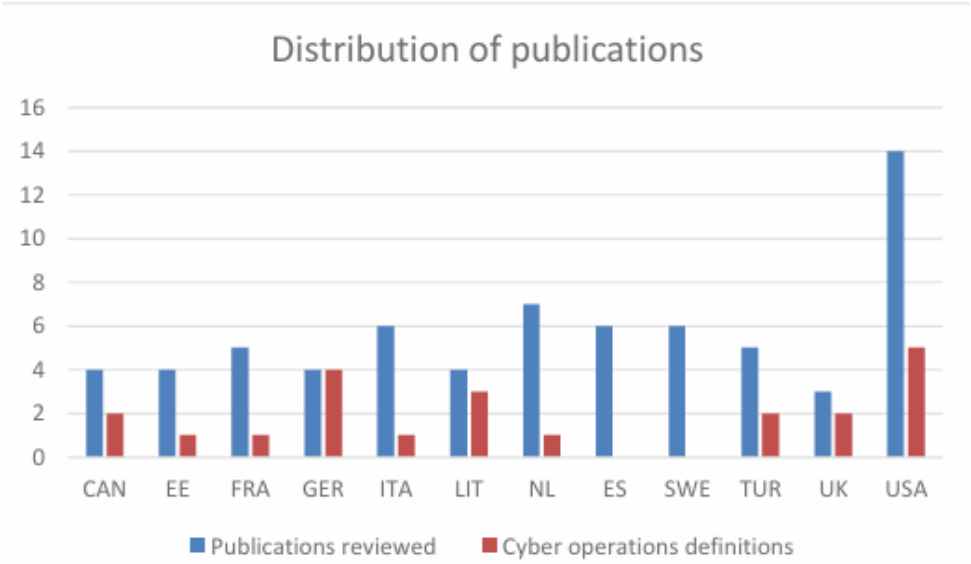

Figure 2. Distribution of NATO Cyber Operations Doctrinal Publications[5]

NATO's involvement in cyber defence demonstrates that the Alliance operates in cyberspace and that cyber defence is a fundamental part of its core mission, collective defence. It is emphasized that NATO is fully aware of the negative effects cyberattacks can have on the vital infrastructures of its member states. NATO's primary responsibility is to defend its Allies against security threats across all domains, including cyberspace. Cyber defence within NATO is not limited to the protection of its own infrastructure; rather, it extends to a broader mission of collective defence of its members. Beyond detecting and countering cyberattacks, this effort includes strengthening the cyber resilience of member states through the sharing of knowledge, experience, and best practices. To support cooperation among member states and international partners, the Alliance has developed a series of policies and strategies that encourage collaboration. This fosters a coordinated and unified response to cyber threats. NATO recognizes the harmful impact cyberattacks can have on critical infrastructures such as financial systems,

[1] Damjan Strucl, *Comparative Study on the Cyber Defence of NATO Members States*, CCDCOE NATO Cooperative Cyber Defence Centre of Excellence Tallin, 2021, p. 3
[2] *Ibidem*, p. 21
[3] Alexander Klimburg (Ed.), *National Cyber Security Framework Manual*, NATO CCDCOE Publication, 2012, pp. 12-13; Miguel Ferreira da Silva, *Cyber Security vs. Cyber Defense: A Portuguese view in the distinction*, Cyberlaw CIJIC, pp. 1-2
[4] Jeppe Jacobsen, *Cyber Offence in NATO: Challenges and Opportunities*, "International Affair", March 2021, p. 3
[5] Marko Arik, *How Do NATO Members Define Cyber Operations?,* "Communications in Computer and Information Science, December 2023, DOI: 10.1007/978-3-031-49212-9_2, pp. 4-5

emergency services, communication networks, and other essential aspects of modern life. Thus, cyber defence is seen not only as a technical necessity but also as a key element of both national and international security[1].

NATO`s Cybersecurity Strategy within the Strategic Concepts

The early 2000s marked a watershed moment in the historical trajectory of cybersecurity within the North Atlantic Treaty Organization (NATO), a period during which the organization began to acknowledge and address cyber threats as substantial risks to both national and international security. Foremost among the drivers of this shift was the heightened awareness prompted by the rapid pace of technological advancement and the widespread proliferation of the Internet, both of which fundamentally altered the dynamics of interstate interaction and defense, not only in terms of self-protection but also in safeguarding allied interests. A seminal step in this evolving posture was the establishment, in 2002, of the Ad Hoc Working Group on Cyber Incident Response, a strategic initiative born out of the pressing need for coordinated action and rapid response to cyber incidents with the potential to undermine the critical infrastructures of NATO and EU member states[2]. This initiative emerged as a direct response to the pressing need for coordination and rapid reaction in the face of cyber incidents, which carried the potential to significantly compromise the critical infrastructures of European Union member states. Its core objective was to establish a robust framework for the exchange of information and best practices among NATO member states, with the overarching aim of enhancing collective defence mechanisms against the escalating tide of cyber threats.

Moreover, the cultivation of awareness across the Alliance was prominently emphasized as a strategic priority, with particular focus placed on educational and training dimensions within the cybersecurity domain. This educational approach was conceived not merely as a transfer of knowledge, but as a comprehensive strategy for fostering specialized competencies and developing the institutional capacities required to effectively confront the multifaceted and evolving spectrum of threats within cyberspace[3]. The current decade has witnessed the evolution of incident response capabilities from relatively modest initial efforts to the formulation of complex and multifaceted strategies that encompass not only reactive measures, but also proactive dimensions of prevention and detection. In alignment with this trajectory, NATO's initiatives have been meticulously designed to ensure effective collective defence, the safeguarding of critical infrastructure, and the sustained functioning of societal life and essential services for citizens[4].

At the NATO Summit held in Bucharest in April 2008, cybersecurity was officially acknowledged as a strategic domain within the framework of the Alliance's collective security architecture. This formal recognition stemmed from an enhanced understanding of the profound international repercussions that cyber vulnerabilities could engender—ranging from the compromise of a state's critical infrastructure to broader implications for global security. The summit adopted concrete measures aimed at strengthening cyber defense and integrating this dimension into both NATO's military and civilian planning processes. In doing so, it laid the foundational groundwork for subsequent policy development and strategic initiatives in the field of cybersecurity[5]. In May 2007, one year prior to the Bucharest Summit, Estonia became the target of a large-scale cyberattack that effectively paralyzed the country's vital infrastructure, including government institutions, financial systems, and mass media outlets. The attacks were precipitated by a diplomatic and social conflict surrounding the relocation of a Soviet-era monument in Tallinn. This incident starkly illustrates the extent to which modern states are vulnerable to cyberattacks and how such operations can severely disrupt the normal functioning of society. The event holds significant importance in the context of NATO's cybersecurity posture, as it served as a critical catalyst in accelerating the recognition of cybersecurity as an essential component of both national and international security

[1]Darius-Antoniu Ferenț, Corneliu Preja, *NATO's involvement in Cyber Defense,* https://www.intelligenceinfo.org/natos-involvement-in-cyber-defence/ (27.03.2025)
[2]NATO, *Cyber defense*, https://www.nato.int/cps/en/natohq/topics_78170.html (27.03.2025)
[3]*Idem*
[4]Kenneth Geers, *Cyberspace and the Changing Nature of Warfare din 2008*, https://ccdcoe.org/uploads/2018/10/Geers2008_CyberspaceAndTheChangingNatureOfWarfare.pdf (27.03.2025)
[5]MAE, *Summit-ul NATO de la București din 2-4.04.2008*, https://www.mae.ro/node/1574 (27.03.2025)

frameworks[1]. The cyberattacks in 2007 Estonia drew full political attention of NATO. A direct conventional attack on Estonia would precipitate NATO's collective 157 military response. However, the lack of provisions at that time made these attacks unpunished. The Estonian Defense Minister Aaviksoo pointed out this aspect: "At present, Nato does not define cyber-attacks as a clear military action. This means that the provisions of Article V of the North Atlantic Treaty, or, in other words collective self-defense, will not automatically be extended to the attacked country"[2]. These attacks served as a wakeup call for NATO's cyber defense capabilities. The development of NATO's cybersecurity policy was significantly shaped by both the 2007 cyberattacks on Estonia and the subsequent formal recognition of cybersecurity at the 2008 Bucharest Summit. These events catalysed collective action and laid the foundation for enhanced cooperation within the Alliance, emphasizing the critical importance of prevention, detection, and response in the face of cyber threats. The decisions taken during these pivotal moments have deeply influenced NATO's approach to cybersecurity, establishing it as a core element of the Alliance's broader security strategy to confront 21st century threats.

In response to the continuously evolving nature of cyber threats, these initiatives underscore the necessity of a proactive and adaptive posture. Nevertheless, despite rapid technological advancements, cybersecurity had not traditionally occupied a prominent place on NATO's strategic agenda. It took a high-profile event such as the cyber assault on Estonia to elevate the issue to the level of a major strategic priority. Further cyberattacks, particularly those that fuelled the crisis in Ukraine's Crimea and Donbas regions, served as an unmistakable wake-up call. At the 2014 Wales Summit, NATO declared a state of heightened alert, placing cybersecurity at the forefront of its political agenda. The Allies endorsed a revised Cyber Defence Policy, and an accompanying Action Plan designed to address the shifting nature of cyber threats. This marked the emergence of a more inventive and forward-looking approach to collective defence in the digital era, positioning cybersecurity at the very heart of NATO's strategic vision[3].

Regarding cybersecurity, NATO achieved significant progress at the 2016 Warsaw Summit. The Allies decisively concluded that the operationalization of cyberspace would henceforth be integrated as a fundamental component of NATO's defense and planning policy, on par with the terrestrial, maritime, and aerial domains[4]. The NATO Cyber Defence Commitment, a significant outcome of the Warsaw Summit, stipulated that NATO member states prioritize the enhancement of cyber defence capabilities for their national infrastructures and networks. Following this mandate, most member states have reviewed or developed comprehensive national cyber defence strategies. These policy developments have engendered workshops, training courses, and exercises aimed at improving the resilience, expertise, and operational capacities of Allies within the cyber domain.

A particularly notable initiative in this regard is the "Locked Shields" exercise, the largest and most sophisticated international live-fire cyber defence exercise. It is organized annually in Tallinn, Estonia, by the NATO Cooperative Cyber Defence Centre of Excellence. Locked Shields gather cybersecurity experts from NATO partner countries, member states, and industry with real-time, scenario-based cyberattacks. This immersive exercise enables participants to practice aspects of defending information technology networks and systems, under realistic conditions. Furthermore, NATO's annual Crisis Management Exercise (CMX) now incorporates crisis scenarios related to cyber warfare and hybrid warfare. Within CMX, both military and civilian of the Alliance test consultation and decision-making processes within realistic simulations based on scenarios derived from Articles 4 and 5 of the NATO Treaty. Presently, these exercises, alongside other initiatives such as the annual Cyber Coalition exercise, play a crucial role in enhancing NATO's collective cyber defence capabilities[5].

---

[1]Rain Ottis, *Theoretical Model for Creating a Nation-State Level Offensive Cyber Capability din 2007*, https://ccdcoe.org/uploads/2018/10/Ottis2009_TheoreticalModelForCreatingANation-StateLevelOffensiveCyberCapability.pdf (27.03.2025)

[2] The Guardian. (2007, May 17). "Russia accused of unleashing cyberwar to disable Estonia", https://www.theguardian.com/world/2007/may/17/topstories3.russia (10.04.2025)

[3]Ulrich Karock, *NATO after the Wales Summit: Back to Collective Defense din 2014*, https://www.europarl.europa.eu/RegData/etudes/BRIE/2014/536430/EXPO_BRI%282014%29536430_EN.pdf (27.03.2025)

[4]CCDCOE, *NATO Recognizes Cyberspace as a 'Domain of Operations' at Warsaw Summit din 2016*, https://ccdcoe.org/incyder-articles/nato-recognises-cyberspace-as-a-domain-of-operations-at-warsaw-summit/ (27.03.2025)

[5]Bruno Lete, Dalga Dege, *NATO Cybersecurity: A Roadmap to Resilience din 2017*, https://www.jstor.org/stable/resrep18857?searchText=NATO+and+Cybersecurity&searchUri=%2Faction%2FdoBasicSearch

In accordance with the NATO-EU Joint Declaration from the Warsaw Summit[1], NATO has also been actively advocating for the intensification of its cooperation with the European Union in the field of cyber defence, recognizing the mutual interest of both entities in enhancing resilience. In February 2016, NATO and the EU formalized this collaboration by signing a technical agreement on cyber defence, aimed at improving communication, cooperation, and information exchange between NATO's Computer Incident Response Capability (NCIRC) and the EU's Computer Emergency Response Team (CERT-EU). Moreover, the European Union has regularly participated in NATO's cyber defence exercises, further solidifying this partnership. Furthermore, NATO increasingly acknowledges the critical importance of collaboration with industry partners to enable the Alliance to fulfil its cyber defence policy objectives. The NATO Industry Cyber Partnership was inaugurated in September 2014 as a strategic initiative to foster closer engagement with the private sector in addressing cyber threats[2]. This initiative signifies the imperative for NATO and industry to collaborate more closely in combating cyber threats through the exchange of information, expertise, and best practices. A strategic partnership between NATO and the EU, the cooperation in the complementary development of defense and security capabilities and the cohesion and efficiency of NATO and EU, and transnational connections are important factors[3] that could contribute to the proper development of the strategic interest in the cyber security field.

NATO cannot afford complacency or optimism in the face of the transformative challenges posed by the digital era. The Alliance is now poised for a critical test and, in this regard, remains in a comparatively precarious position to manage the rapid changes that cyberspace has introduced to the security domain. In the eyes of its members, partners, and adversaries alike, NATO must consolidate its standing as a robust and formidable force within the cyber environment. To achieve this imperative, NATO must persist in enhancing its cyber force multiplication capabilities, refine its command and decision-making systems to operate effectively during cyber crises and conflicts, and bolster interoperability with cyber allies and partners. Swift responses to contemporary security challenges demand flexible policy frameworks that empower networked actors with the discretion to employ coercive measures as appropriate.

In alignment with the emerging digital world order, NATO's forthcoming high-level summits must continue to evolve and adapt the Alliance's posture and strategic orientation[4].

Article 5 in the Context of Cybersecurity

Even though the application of Article 5 of the Alliance is characterized by flexibility in the application process, as an essential aspect of the Alliance` integrity, it also could create some specific uncertainties in the terms of cyberspace. Article 5 refers to the Principle of Individual or Collective Defense, and states that "an armed attack against one or more [parties] in Europe or North America shall be considered an attack against them all [which then] will assist the Party [by taking] such action as it deems necessary […] to restore and maintain the security of the North Atlantic area"[5].

At the 2021 NATO Summit in Brussels, member states adopted a Comprehensive Cyber Defence Policy aimed at reinforcing NATO's three core tasks and strengthening its overall deterrence and defence posture. They reaffirmed NATO's defensive role and pledged to use the full spectrum of capabilities to deter, defend against, and respond to the entire range of cyber threats—potentially through collective action. These responses must be continuous and utilize the full breadth of NATO's instruments, including political, diplomatic, and military tools.

%3FQuery%3DNATO%2Band%2BCybersecurity%26so%3Drel&ab_segments=0%2Fbasic_search_gsv2%2Fcontrol&refreqid=fastly-default%3A03d70d1e89a7f472381c8f454036a6c9&seq=1, (11.03.2025)

[1]Consiliul European, *Summitul NATO, Varşovia, Polonia, 8-9.07.2016*, https://www.consilium.europa.eu/ro/meetings/international-summit/2016/07/08-09/ (25.03.2025)

[2]Bruno Lete, Dalga Dege, *NATO Cybersecurity: A Roadmap to Resilience din 2017*, https://www.jstor.org/stable/resrep18857?searchText=NATO+and+Cybersecurity&searchUri=%2Faction%2FdoBasicSearch%3FQuery%3DNATO%2Band%2BCybersecurity%26so%3Drel&ab_segments=0%2Fbasic_search_gsv2%2Fcontrol&refreqid=fastly-default%3A03d70d1e89a7f472381c8f454036a6c9&seq=1 (17.03.2025)

[3] Rajnai Zoltan, Dai Phuoc Huu Nguyen (Eds.), *Cyber Security*, L`Karmattan, Paris, 2023, pp. 25-27

[4]*Idem*

[5] North Atlantic Treaty Organization, *The North Atlantic Treaty,* https://www.nato.int/cps/en/natohq/official_texts_17120.htm (10.03.2025)

Allies also acknowledged that the cumulative effect of significant malicious cyber activities could, under certain conditions, be considered an armed attack, potentially prompting the North Atlantic Council to invoke Article 5 on a case-by-case basis. Given the complex nature of cyberspace, a unified and comprehensive approach is essential across political, military, and technical dimensions. The 2021 policy, along with its action plan, guides NATO's efforts across all three levels.

Despite NATO's recognition of the critical importance of enhancing cyber capabilities, significant ambiguities and challenges persist. A fundamental issue concerns the ambiguity surrounding the application of Article 5 in the context of cyberattacks, raising complex questions regarding the threshold at which a cyber incident qualifies as an "armed attack" warranting a collective response. Myriam Dunn Cavelty further highlights the risk that NATO may overextend its mandate in the cyber domain, potentially exceeding its capacity and available resources. The author consider that NATO needs to avoid its article 5 aspirations for cyberattacks and risks taking on too much cybersecurity accountability[1].

To build a resilient and adaptive cyber defence posture, NATO members and international partners must foster closer cooperation and robust information sharing. It is imperative to underscore the necessity for a coordinated and balanced approach to effectively address cyber threats, emphasizing the continuous adaptation of NATO's strategies to the rapidly evolving security environment[2].

NATO remains firmly committed to upholding international law, including the UN Charter, international humanitarian law, and international human rights law, where applicable. The Alliance continues to advocate for free, open, peaceful, and secure cyberspace, while advancing efforts to strengthen stability and minimize the risk of conflict. This includes promoting respect for international legal frameworks and supporting voluntary norms for responsible state behavior in cyberspace[3]. The problem of ensuring the security of information technologies and systems of NATO and its members has, in addition to issues of technical support and strategic planning, a political dimension. First, this refers to the possibility of applying Article 5 of the Founding Treaty in relation to information attacks. The most active protagonists of the expansion of the principle of collective responsibility in the field of information security are Estonia and, partially, the USA[4]. Some authors consider that by not releasing the terms of the policy (related to the NATO Space Policy as classified) the alliance doesn't clearly outline how and if the Article 5 protections apply to space assets[5]. The question is if an attack via cyber means may be considered an armed attack, as it may not be executed through traditional, physical armed forces. In this context it is important to additionally refer to Article 6, the Nationality Principle – an attack is only recognized if "deemed to include an armed attack on the territory of any of the Parties (…) in the forces, vessels, or aircrafts of any of the Parties, when in or ever these territories or any other area"[6]. Also, we need to mention that NATO`s cyber defense actions are framed within article 4 – members will consult together in the case of cyber-attacks, even though are not duty bound to aid each other as it is described in Article 5. "Keeping NATO's cyber defense within Article 4 mechanisms is in fact crucial if NATO wants to remain a credible player in cybersecurity matters—anything else would lead to severe legal, practical, and strategic problems. However, it is very likely that there will be further attempts to move the

[1] Myriam Dunn Cavelty, *Cyber-Allies. Strengths and Weaknesses of NATO`s Cyber Defence posture*, IP Global Edition, Vol. 12, No. 3, p. 11

[2]Myriam Dunn Cavelty, *Cyber-Allies: Strengths and Weaknesses of NATO's Cyber Defense Posture* https://www.researchgate.net/publication/228199410_Cyber-Allies_Strengths_and_Weaknesses_of_NATO's_Cyberdefense_Posture (27.03.2024)

[3] North Atlantic Treaty Organization, *Cyber Defense*, 30th of July 2024, https://www.nato.int/cps/en/natohq/topics_78170.htm#:~:text=At%20the%202021%20NATO%20Summit%20in%20Brussels%2C%20Allies,well%20as%20its%20overall%20deterrence%20and%20defence%20posture.

[4] Paul Neuman, *NATO and Cyber Security,* https://www.researchgate.net/publication/352107026_NATO_and_Cyber_Security (12.04.2025)

[5] Myriam Dunn Cavelty, *Cyber-Allies. Strengths and Weaknesses of NATO`s Cyber Defence Posture*, IP Global Edition, Vol. 12, No. 3, p. 14

[6] North Atlantic Treaty Organization, *The North Atlantic Treaty,* https://www.nato.int/cps/en/natohq/official_texts_17120.htm (10.03.2025)

cyber topic under the frame of Article 5"[1]. If we add at those already mentioned in this context the 2022 Albanian incidents, that spurred renewed discussions on how Article 5 ought to apply in cybers space[2].

Conclusions

Over time, the Alliance has implemented initiatives and measures to enhance the cyber defense capabilities of its member states and ensure a coordinated response to cyberattacks. NATO has recognized the critical importance of cybersecurity and has developed comprehensive policies and institutional frameworks to address these emerging threats. Cyberspace has become an essential operational domain for NATO, prompting the Alliance to adapt and respond to these emerging security challenges. Founded on the principle of collective defence, the North Atlantic Alliance has consistently demonstrated a capacity for adaptation to effectively address evolving threats to the security of its member states. A significant shift in NATO's security doctrine was the formal recognition of cyberspace as a distinct operational domain, on par with the traditional domains of land, air, and sea. This strategic reorientation underscores the critical importance of cyberspace and NATO's commitment to safeguarding the vital digital infrastructures of its members against cyberattacks. NATO possesses sophisticated mechanisms that enable member nations to collaborate and coordinate effectively to ensure robust cyber defense.

These mechanisms, including Center of Excellence, rapid response teams, and unified cybersecurity policies are specifically designed to facilitate swift and coordinated reactions to cyber threats. Major cyber incidents, such as attacks targeting vital infrastructure within member states, have exposed existing vulnerabilities and underscored the necessity of a cohesive and efficient approach to managing such threats. These events have brought to light the imperative of implementing a common strategy and fostering international cooperation to respond effectively to the complex challenges of the cyber domain. In an increasingly digitalized world, cybersecurity has become a fundamental component of both national and international security.

The protection of critical infrastructure and sensitive data from cyber threats has gained prominence over recent decades, leading to the emergence and evolution of the cybersecurity paradigm. Cyber threats have far-reaching implications, impacting the global economy, public health systems, and national security. Vulnerabilities within cyber infrastructure can result in significant financial losses, erode public trust, and pose substantial risks to public health and safety. Strengthening cybersecurity requires robust international cooperation.

To establish common security standards and facilitate the exchange of information and best practices, NATO actively engages with other international organizations, such as the European Union, as well as with non-member states. Current trends underscore the urgent need for a cybersecurity posture that is both resilient and adaptable. Threats such as ransomware, phishing, and the deployment of automation and AI in cyberattacks exemplify the dynamic nature of the cyber domain. NATO has long acknowledged the importance of cybersecurity and has established policies and institutional structures aimed at countering these risks. Over time, the Alliance has implemented a range of initiatives and measures to enhance the cyber defences of its member states and ensure a cohesive and coordinated response to cyberattacks. High-profile cybersecurity incidents such as attacks on healthcare systems and critical infrastructure have demonstrated the extent to which contemporary society remains exposed to digital vulnerabilities. These threats are continuously evolving, becoming increasingly complex and sophisticated.

Bibliography

Books

1. Czosseck, Christian; Geers, Kenneth (Eds.), *The Virtual Battlefield: Perspectives on Cyber Warfare,* IOS Press, Amsterdam, Berlin, Tokyo, Wahington, DC, 2009
2. Kitabi, Bildiri, *On the Individual, Society, and Politics in a Digitalized World*, Ivik University, Istanbul, 2022
3. Klimburg, Alexander, (Ed.), *National Cyber Security Framework Manual*, NATO CCDCOE Publication, 2012

[1] Myriam Dunn Cavelty, *Op. cit.,* p. 14
[2] Sarah Wiedemar, *NATO and Article 5 in Cyberspace*, "CSS Analyses in Security Policy", No. 323, May 2023, p. 2

4. Strucl, Damjan, *Comparative Study on the Cyber Defence of NATO Members States*,

Articles and Studies

1. Arik, Marko, *How Do NATO Members Define Cyber Operations?,* "Communications in Computer and Information Science", December 2023
2. Cavelty, Dunn, Myriam, *Cyber-Allies. Strengths and Weaknesses of NATO`s Cyber Defence posture*, IP Global Edition, Vol. 12, No. 3
3. Gjoreski, Igor; Nacev, Zoran, *Global Security Trends in Euro-Atlantic Area and NATO New Strategic Concept,* "Security Dialogues", Vol. 13, No.2, 2022
4. Halili, Albulena, *Non-traditional Security Threats and NATO`s Response in the Contemporary Security Environment*, "SEEU Review", Vol. 18, No. 2, 2023
5. Jacobsen, Jeppe, *Cyber Offence in NATO: Challenges and Opportunities*, "International Affair", 2021
6. Wiedemar, Sarah, *NATO and Article 5 in Cyberspace*, "CSS Analyses in Security Policy", No. 323, 2023

Documents

1. North Atlantic Treaty Organization, *Cyber Defense*, 30th of July 2024
2. Research Division NATO Defence College Rome, *Strategic Shifts and NATO`s New Strategic Concept,* NATO Defense College, Rome, 2022
3. CCDCOE, *NATO Recognizes Cyberspace as a 'Domain of Operations' at Warsaw Summit din 2016*
4. North Atlantic Treaty Organization, *The North Atlantic Treaty*
5. CCDCOE NATO, *Cooperative Cyber Defence*, Centre of Excellence Tallin, 2021

Internet

1. https://www.act.nato.int/
2. https://www.nato.int/
3. https://ccdcoe.org/
4. https://www.intelligenceinfo.org/
5. https://www.mae.ro/
6. https://www.theguardian.com/
7. https://www.europarl.europa.eu/
8. https://www.jstor.org/
9. https://www.consilium.europa.eu/