NATO AS A GLOBAL CYBERSECURITY POWER

Gökhan Tekir[1], Ankara Hacı Bayram Veli University

ABSTRACT

The landscape of threats has been undergoing a tremendous change. As the state institutions, infrastructure providers, banks, and companies operate in cyber realm, the security of this realm has become increasingly a main facet of the national security. Even military operations have been entrenched in cyber operations with the articulation of new concepts such as hybrid warfare. US Department's recognition of attacks on computer networks as an act of war demonstrates the relevance of cybersecurity to security of the states. Similarly, North Atlantic Treaty Organization (NATO) included cyberspace as the fourth domain besides air, land, and sea in 2016. Digital authoritarianism promoted by China for the aim of spreading its digital norms across the world and hybrid warfare promulgated to disrupt the stability of the countries located in the post-Soviet space necessitates NATO's active involvement in cybersecurity realm. In 2021, it unveiled an ambitious NATO 2030 agenda in which NATO positioned itself a global competitor against rising threat of cyberattacks. Since Internet and cyber networks are inherently transnational, responding to cyberthreats requires a global approach. Thus, defining cybersecurity as a priority area is an important step in transforming NATO from a regional organization to a global one. This study aims at examining NATO's endeavors to tackle cyberthreats and its evolving role in the global arena. The members' positions in setting up a common approach concerning cybersecurity will determine NATO's transformation into a global security actor.

Keywords: NATO, cybersecurity, cyberspace

Introduction

So far the 21st century has been shaped by the developments in internet networks. Due to rapid technological change digital communication has an enormous impact on the organization of society, economy, and politics. People from various parts of the world are connected through the Internet, making the distances meaningless. The private companies and financial institutions perform their operations in cyberspace, trying to achieve fastness and excellence in their services. The states also started to use digital technology from providing services to their citizens to military and intelligence activities.

As digital technologies and human lives become extremely intertwined, the security of the digital platforms is as vital as physical infrastructure of the states. The attacks on cyberspace could have devastating effects on society that could be similar to conventional war. Thus, the protection of cyberspace has developed into one of the priority areas for the states.

[1]Assist. Prof., Department of International Relations. E-mail: gokhan.tekir@hbv.edu.tr

The North Atlantic Treaty Organization (NATO) recognized cyberspace as a significant part of collective defense. Since 2016, cybersecurity is a domain of operations alongside land, air, and sea. Although each NATO member is encouraged to develop its own national cybersecurity agendas, collectively it is NATO's duty to organize and coordinate security of cyberspace and common response to cyberattacks to NATO members. Especially Russia's increasing reliance on cyberattacks with the hybrid war doctrine and the activities of China-associated hackers on private and official networks have enhanced the role of NATO. The nature of cyberattacks compels NATO to evolve from regional to global organization. As cyberattacks transcend nation state boundaries, NATO needs global conception to deal with these threats. Playing a leading role in establishing relations with global partners from private or international organizations in various areas of the world and operation centers would transform NATO into a global cybersecurity provider in the world. In order for this transformation to occur, political and legal background that defines NATO's cybersecurity role must be provided besides technical expertise.

Cyberattack and Cybersecurity

In Talinn Manuel on the International Law Applicable to Cyber Warfare, cyberattack is defined as "cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects " (Schmidt, 2005: 106). U.S. Department of Defense describes cyberattack as

> "A hostile act using computer or related networks or systems, and intended to disrupt and/ or destroy an adversary's critical cyber systems, assets, or functions. The intended effects of cyber attack are not necessarily limited to the targeted computer systems or data themselves-for instance, attacks on computer systems which are intended to degrade or destroy infrastructure or C2 capability. A cyber attack may use intermediate delivery vehicles including peripheral devices, electronic transmitters, embedded code, or human operators. The activation or effect of a cyber attack may be widely separated temporally and geographically from the delivery" (*Cyberspace Operations Lexicon*: 5).

Germany considers cyberattack as an attack in cyberspace aiming to damage cyberspace's confidentiality, integrity, and availability (Hathaway & Klimburg, 2012: 18). According to NATO, cyberattack is "an act or action initiated in or through cyberspace to cause harmful effects" (*AAP-06 Edition 2021*, 2021: 37).

These four definitions overlap and differ with each other. The overlapping element is that all four definitions consider cyberattack as disruption of cyberspace. On the other hand, the Tallinn

Manual restricted the context of cyberattacks in armed conflicts. The emphasis on this definition is on the use of force by defining cyberattacks "cause injury or death to persons or damage or destruction to objects." The definition of cyberattacks by the U.S. Department of Defense focuses on sabotage to "critical cyber systems, assets, or functions." Germany's definition contains attacks on confidentiality, evaluating cyberespionage as cyberattacks. The broader description has been made by NATO. Cyberattacks are acts that "cause harmful effects." The harmful effects in cyberspace include cybercrimes and cyberterrorism activities perpetrated by states to non-state actors.

Cyberterrorism is defined by security expert Dorothy Denning as "politically motivated hacking operations intended to cause grave harm such as loss of life or severe economic damage." The Federal Emergency Management Agency (FEMA) designates cyberterrorism as "unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives" (Wilson, 2008: 4). Cybercrime includes offenses ranging from hacking computer data and systems, computer-related forgery and fraud to content offenses (such as child pornography) and copyright offenses (United Nations Office on Drugs and Crime, 2010). Considering the transnational nature of cybercrime, evidence is located across various locations in the world. Many law enforcement agencies do not have the capability to conduct investigations about cybercrime related offenses, which threaten the citizens and infrastructure (INTERPOL, n.d.). The transnational aspect of cyberspace, therefore, complicates the ways to cope with cyberattacks. In this environment, it becomes extremely difficult to maintain security in cyberspace. Cybersecurity is defined as:

> "the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment" (*Introduction to Security Cyberspace, Cybercrime and Cybersecurity*, n.d.).

NATO uses two different terms that are related with cybersecurity. The first is information security environment which refers to communications and information systems (CIS) security. Security means "the ability to adequately protect the confidentiality, integrity and availability of CIS and the information processed, stored or transmitted." The second term is cyber defense

defined as: “the ability to safeguard the delivery and management of services in an operational CIS in response to potential and imminent as well as actual malicious actions that originate in cyberspace” (Hathaway & Klimburg, 2012: 12–13). To cope with radically changed security environment in cyberspace, NATO has taken important steps in cybersecurity.

Overview of NATO’s Measures Against Cyberattacks

The first cyber crisis that NATO encountered occurred in its Kosovo air campaign in 1999. NATO’s e-mail account was blocked, and NATO’s website was disrupted. At that time, cyber dimension of the conflict was considered subordinate to conventional warfare. Only technical responses were thought to be adequate to respond to these attacks (Theiler, 2011). The political and security aspect of cyberattacks in 1999 were overlooked.

The cyberattacks in 2007 Estonia drew full political attention of NATO. The attacks on Estonia started on April 27, 2007, and ended on May 18, 2007. The problem arose from the dispute concerning the Soviet memorial of bronze statue of a soldier. When Estonian government decided to move the statue, the hostile actions provoked by the Russian state began. The Estonian embassy was sieged, and the Estonian ambassador was physically harassed. In Estonia, cyberattacks consisted of three phases. The first phase of attacks targeted government websites, through straightforward ping command. The employment of malformed web queries against government websites followed. The second phase of attacks, started on May 4, involved intense and certain attacks against websites and data name servers. The attacks intensified on May 9, which is the date of Russia’s Victory Day. The DDoS attacks increased by 150 percent on May 9 and May 10. In the third wave of attacks, 85,000 computers were hijacked from noon to midnight on May 15. Estonia’s largest bank Ühisbank, other banks and government agencies were preys of cyberattacks (Buresh, 2021: 16). These cyberattacks could be considered as acts of cyberterrorism which targeted public services, commerce, and government operations. Estonian Defense Minister Jaak Aaviksoo observed that successful cyberattacks "can effectively be compared to when your ports are shut to the sea." (Herzog, 2011: 54). Although the Russian Federation denied involvement, these cyberattacks were accompanied with very hostile rhetoric of Russian state officials, their refusal of cooperation with Estonian officials, and the imposition of economic measures (NATO StratCom, n.d.). Thus, Russia emerges as a usual suspect for these attacks. The cyberattacks on Estonia, indeed, a cost-effective attack for Russia to punish Estonia, a former republic of the Soviet Union, which seeks to assert its rightful sovereignty. A direct conventional attack on Estonia would precipitate NATO’s collective

military response. However, the lack of provisions at that time let 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" (The Guardian, 2007). Yet, these attacks served as a wake-up call for NATO's cyber defense capabilities.

In 2011, during its Libyan operation, NATO had to deal with cyberattacks from hacktivists. Although there was no direct relationship found between the the Libyan operation and cyberattacks, the timing of these attacks could not be coincidental. Anonymous, a well-known hacktivist group infiltrated into the NATO server and extracted a large amount of data. LulzSec, another hacker group, intruded NATO server and released the names, usernames, and passwords of the registered users. When NATO's operation started, a software attack targeted the Norwegian military. The NATO Computer Incident Response Capability (NCIRC) created in 2002 at the Prague Summit defended these malicious cyberattacks (Healey, 2011). However, the continuing cyberattacks during NATO's military engagements demonstrate that the absence of a political stance in NATO regarding cyberattacks invited these cyberattacks, which would harm the digital infrastructure of NATO countries that cannot be confronted militarily.

The 2010 NATO Strategic Concept raised the issue of addressing cyberattacks by pointing out the need to "develop further our ability to prevent, detect, defend against and recover from cyber-attacks…" (NATO, 2011a). In June, Defense Ministers from NATO countries adopted a new cyber defense strategy which rested on three pillars: prevention, coping with cyberattacks, and limiting their impact. Then- NATO Secretary General, Anders Fogh Rasmussen stated: "*A well-orchestrated cyber attack can turn off the power in your house, your city, your country. It can shut down air traffic control. It can shut down banks. In short, a cyber attack can bring a country down without a single soldier having to cross its borders It is no exaggeration to state that cyber attacks have become a new form of permanent, low-level warfare" (NATO, 2011b). This description of cyberattacks as low-level warfare was an important step in NATO's subsequent policies concerning cyber defense.*

In April 2012, cyber defense was included in the NATO Defense Planning Process. In 2012, at the Chicago Summit the leaders of NATO countries affirmed their commitment to improve NATO's cyber defense capabilities. They concluded the centralized protection of NATO networks. In July 2012, the NATO Communications and Information Agency was established

(NATO, 2022). In 2014, at the Wales Summit, NATO adopted enhanced policy and action plan on cyber defense, which established cyber defense as a core part on NATO's collective defense, affirming that international law applies in cyberspace and increasing NATO's engagement with the industry. The policy also outlined streamlined cyber defense governance, assistance to NATO countries, which would experience cyberattacks, and operational planning on cyber defense. This policy also touches upon raising awareness, education, exercises, training, and cooperation (NATO, 2016a).

The most striking development in NATO's policy concerning cyberspace occurred in 2016 at the NATO Summit in Warsaw. The NATO countries issued a cyber defense pledge, recognizing cyberspace as the fourth domain of operations. The first article of the pledge states: "In recognition of the new realities of security threats to NATO, we, the Allied Heads of State and Government, pledge to ensure the Alliance keeps pace with the fast evolving cyber threat landscape and that our nations will be capable of defending themselves in cyberspace as in the air, on land and at sea" (NATO, 2016b). This confirmation has important consequences. Considering cyberspace as an operational domain enables NATO to prepare a better framework to protect its missions and operations, focusing on training and military planning. It helps NATO manage its resources, skills, and capabilities (NATO, 2016a). NATO countries pledge to enhance their own cyber defense capabilities in their digital infrastructures and deepen their cooperation in defending cyberspace (NATO, 2016b). As the most successful defensive alliance in the world history, the inclusion of cyberspace into an operation of domain would present a formidable deterrence to cyberattacks against NATO countries' cyberspace.

In 2018, NATO Summit in Brussels declared: "Reaffirming NATO's defensive mandate, we are determined to employ the full range of capabilities, including cyber, to deter, defend against, and to counter the full spectrum of cyber threats, including those conducted as part of a hybrid campaign" (NATO, 2018). At this summit, a new Cyberspace Operations Centre was established, which aims to raise situational awareness of Allied countries and coordinates NATO's operational activity in and through cyberspace. In February 2019, Defense Ministers of NATO accepted a set of measures including political, diplomatic, and military ones to protect NATO's cyberspace (NATO, 2022).

The COVID-19 pandemic raised the importance of cyberspace as most of economic, political, educational, or other activities have been moved to cyberspace due to pandemic closures. In June 2020, the North Atlantic Council issued a statement which condemns malicious cyber

activities and calls for responsible state behaviors (NATO, 2022). 2021 NATO Brussels Summit Communique reaffirms NATO's commitment to protect NATO's three core tasks of collective defense, crisis management, and cooperative security. Pointing out increasing threats in cyberspace, mostly emanated from Russia, NATO countries endorsed a Comprehensive Cyber Defense Policy. NATO stresses that it is ready to deter, defend against, and counter the full spectrum of cyber threats. It is stated that NATO does not only deal with state sponsored cyberattacks but also other cyber actors' exploitation of the COVID-19 pandemic (NATO, 2021a).

This communique is significant in that NATO emphasized the concept of deterrence to prevent cyberattacks. Deterrence is about stopping undesired actions before they occur. The core of the concept of deterrence is the making of military threats to block actors from making aggressive behaviors (Buzan, 1987: 136). NATO Secretary General Jens Stoltenberg stressed that NATO's integration of cyber defense into military operations signifies "the biggest overall shift in decades" (Arts, 2019). The evolution from defense to deterrence would bolster NATO's power in discouraging hostile actors.

Yet, NATO's ability to respond to cyberattacks depends on the allies' capability in cyberspace. Alliance cyber assets are not NATO owned, but provided by allied states (Arts, 2019). NATO serves as a platform for the Allies to consult, share information, exchange practice, and coordinate activities in cyberspace (NATO, 2021b). The contribution of the US, which has the most sophisticated cyber defense capability among the Allies and a global leader in offensive cyber capabilities is crucial for NATO. In 2018, it announced that it would contribute to bolstering NATO's cyber defense and offense posture. The White House authorized the use of cyber weapons in offensive form to deter foreign adversaries with the publication of the Department of Defense's 2018 Cyber Strategy under the slogan of "Defending Forward." The name suggests a defensive nature by preemptive methods. NATO's following U.S. doctrine and capabilities in cyberspace will reinforce its ability to deal with cyberattacks, which already became elements of hybrid warfare in today's conflicts (Arts, 2019). The adoption of a preemptive approach would help NATO deter cyberattacks and enhance its presence globally to cope with threats that will affect the Allies.

Cyberattack Landscape

NATO has been confronting cyberattacks in a global context. The increasing role of asymmetric warfare highlighted the concept of hybrid warfare. It is defined as "the synchronized use of multiple instruments of power tailored to specific vulnerabilities across the full spectrum of societal functions to achieve synergistic effects" (Cullen & Reichborn-Kjennerud, 2017: 8). Especially Russia employs hybrid war as a main strategic objective to shape the governance and geostrategic orientation of the targeted country (Clark, 2020: 11). Although hybrid warfare is not equated with cyberattacks, cyberattacks constitute key tools of the hybrid warfare. Cyberattacks attract attention and imagination of the public and have tangible, immediate and visible consequences in the physical world (Siman, 2022: 1). Russia's invasion of Eastern Ukraine and its annexation of Crimea in 2014 intensified its efforts in information warfare in cyberspace. Russia views information warfare as a front in which Russia is constantly at a no-peace no-war situation but it is in perpetual state of conflict with the West. Another major attack occurred in 2016 Presidential Election in the USA. Approximately 20,000 e-mails belonging to Hillary Clinton's election headquarters were leaked through Wiki-Leaks to discredit her. The White House officially acknowledge the meddling of Russian hackers as a result of official inquiry. The U.S. director of National Intelligence described Russian covert influence campaign as ambitious and designed to counter U.S. leadership in the global arena (Nocetti, 2018: 182). In its latest invasion of Ukraine started in February 2022, it was expected that cyberattacks would play a critical role. Despite Russia's strong cyber capabilities, its cyberattacks against Ukrainian networks have been limited. The difficulty of conducting large scale cyberattacks in the short-term and Ukraine's capabilities in cyber defense contributed to this outcome. Yet, Russia launched denial of service attacks against Ukrainian defense and banking web sites. Other cyberattacks targeted various Ukrainian government agencies and media institutions (Fendorf & Miller, 2022). An official from NATO warned Russia that cyberattacks against NATO countries would trigger the Article 5 clause of NATO (Pearson & Landay, 2022). The resolution of NATO especially in cyberspace would restrain Russia's behavior in conducting cyber operations against Ukrainian targets and deterring cyberattacks against NATO countries.

In addition to its traditional rival Russia, China and North Korea emerged as the forerunners of the state-sponsored cyberattacks against Western democracies. In April 2020, U.S. Department of State issued a report concerning North Korea's cyber capabilities, warning that these cyber capabilities are used to disrupt U.S. critical infrastructure and steal from financial institutions. In May 2020, the Federal Bureau of Investigation (FBI) and the Cybersecurity and

Infrastructure Security Agency (CISA) concluded that the Chinese government engaged in stealing intellectual property through cyberattacks systematically (Mancuso et al., 2021: 32–33). In July 2021, NATO expressed its concerns directly regarding the challenges that China posed in cyberspace, including the Microsoft Exchange Service Compromise. The President of the NATO Parliamentary Assembly, Gerald E. Connolly condemned cyberattacks conducted by China and China-affiliated groups:

> "NATO Allies took a major step in exposing China's irresponsible behavior in cyberspace and systematic efforts to disrupt and undermine the processes at the heart of our democracies and free economies. Cyber-attacks conducted by the Chinese authorities and their proxies have undermined the security and integrity of networks worldwide and can cause considerable harm to our security, economy, and our democratic societies. I urge China to uphold its international commitments, abide by recognized international norms and stop engaging directly or indirectly in such malicious and criminal cyber operations, which I strongly condemn" (NATO Parliamentary Assembly, 2021).

Despite being geographically distant, the global characteristic of cyberspace makes China relevant to NATO. Increasing Chinese operations in cyberspace to steal industrial and military secrets by hacking computers has raised concerns among NATO members. China has also engaged in disinformation activities in NATO countries. Furthermore, deploying 5G networks across Africa, the Middle East, and Europe has created new security concerns for NATO countries (Erlanger & Shear, 2021). Brussels Summit Communique also identifies China as growing security threat against the NATO alliance, pointing out its activities in cyberspace (NATO, 2021a). Indeed, the cybersecurity firm Check Point Research reported that Chinese oriented cyberattacks have increased 72 percent worldwide since the invasion of Ukraine. Chinese cyberattacks against NATO countries have risen 116 percent during that time (Conklin, 2022). To cope with the rising Chinese threat in cyberspace NATO has to expand its cyber operations in the global scene. This requires establishing relations with international, supranational, and regional organizations and countries across the world.

NATO's Global Partnerships in the Cybersecurity Field

To enhance its cybersecurity capabilities, NATO collaborated with both private sector and global organizations. In September 2014, the NATO Industry Cyber Partnership (NICP) was endorsed at the Wales Summit. Its principles follow as:

- Improve cyber defense in NATO's defense supply chain;

- Facilitate participation of industry in multinational Smart Defense projects;
- Contribute to the Alliance's efforts in cyber defense education, training and exercises;
- Improve sharing of best practices and expertise on preparedness and recovery (to include technology trends);
- Build on existing NATO initiatives for industry engagement, providing specific focus and coherence on the cyber aspects;
- Improve sharing of expertise, information and experience of operating under the constant threat of cyber attack, including information on threats and vulnerabilities, e.g. malware information sharing;
- Help NATO and Allies to learn from industry;
- Facilitate access by Allies to a network of trusted industry/enterprises;
- Raise awareness and improve the understanding of cyber risks;
- Help build access and trust between NATO and the private sector;
- Leverage private sector developments for capability development, and;
- Generate efficient and adequate support in case of cyber incidents (NCIP, n.d.).

NCIP held a two-day conference in Mons, Belgium. 1,500 industry leaders and policymakers attended this conference where they discussed cooperation in cyberspace in 2014 (NATO, 2022). In 2016, NCIP signed a partnership agreement with Fortinet, the global leader in high-performance cybersecurity solutions (Fortinet, 2016). In 2018, NITEC18 conference was held in between the NATO Communications and Information Agency and Vodafone Global Enterprise Limited, AT&T, CY4GATE (an Elettronica Group company) and Thales Communications & Security S.A.S. four new bilateral agreements were signed with leading cyber industry groups on cyber information sharing. These agreements aimed to bolster cyber defense capability, encourage collaboration on cyber threats, and enhance situational awareness in protecting cyberspace (NCI Agency, 2018). In 2019, Science and Technology Committee (SCT) delegation visited the UK National Cyber Security Centre where it held meetings with industrial partners, discussing cybersecurity solutions and innovations in the field (Davis, 2019: 11). NATO also sets up partnership to upgrade its cyber hardware through partnerships with the private sector. The NATO Cyber Security Centre (NCSC) collaborated with industry partners Cisco, RSA, and EuroOne to replace old cyber equipment via a project started in 2019 and ended in 2022 (Savage, 2022). The inclusion of private sector in NATO's cyber defense

capabilities is important in that formidable rivals such as China organizes their private security companies for the goals of the state. An effective counter to these rivals would be mobilizing private sector in NATO countries in the cyberspace.

Besides cyber industry, NATO enhanced its collaboration with other organizations in the world. In February 2016, NATO and the European Union (EU) signed a Technical Arrangement on Cyber Defense to upgrade both organizations' capability to respond cyberattacks. This Technical Arrangement between NCIRC and the Computer Emergency Response Team of the EU (CERT-EU) provides a framework for both parties to exchange information and raise cooperation. In February 2017, NATO and the EU ministers set up cooperation mechanisms in cyber defense including reporting cyberattacks and crisis management (NATO, 2022). NATO and the EU coordinated their operations in cyberspace. In 2017, NATO's Crisis Management Exercise and the EU's Parallel and Coordinated Exercise were conducted at the same time. In 2018, the EU ran a civil-military crisis management exercise in parallel with a NATO staff command-post exercise. (Davis, 2019: 11).

In addition to EU member countries NATO expanded its cooperation with non-EU and non-NATO countries in Europe. In February 2017, NATO and Finland signed Political Framework Arrangement on cyber defense cooperation, which improves the resilience of their cyberspaces (NATO, 2022). Finland also joined Multinational Cyber Defense Capability Development (MNCD2), which is a multinational project to develop security in cyberspace founded by Canada, Denmark, the Netherlands, Norway, and Romania in 2013. Through the MNCD2 the members joined efforts to upgrade cybersecurity capabilities and coordinate scientific and technical capabilities. It also provides a forum for the discussion over the needs of cyber defense, offer recommendations to meet them, and coordination with cyber defense civil entities and private industries (NCI Agency, n.d.). In 2021, NATO held Cyber Coalition 21 exercise to which several cyber defenders from NATO countries and partners Finland, Ireland, Sweden, and Switzerland participated. The scenarios in this exercise included a cyberattack on gas-supply pipelines, a cyberattack which disrupted the logistics of the army, and a cyberattack targeting vaccination programmes (NATO, n.d.). It is striking that NATO invited non-NATO countries to this important exercise which covered energy security to pandemic- related cyberspace security. NATO also established partnerships with Ukraine and Georgia, improving security in their cyberspace. NATO's other partners in cybersecurity area are Moldova, Iraq, and Jordan (Davis, 2019: 12). Thus, NATO's activity in cyberspace transcends NATO borders.

The NATO 2030 agenda calls for strengthening relations with like-minded global partners and form engagements in Africa, Asia, and Latin America. The agenda recognizes the fact that NATO needs to adopt a global approach to tackle global challenges to NATO's security. It also encourages NATO to set international norms and standards in space and cyberspace (NATO, 2021c). The engagement with the four Asia-Pacific partners, which are Australia, Japan, the Republic of Korea and New Zealand, is significant for NATO to address the challenges in the Asia-Pacific region. NATO's global partners have access to full range of NATO's activities. They work with NATO on cross-cutting threats such as cyber defense, resilience, and counter-terrorism (NATO, 2021d). Ukraine increased its cyber defense by collaborating with NATO. NATO Cooperative Cyber Defense Centre of Excellence (CCDCOE) located in Estonia accepted Ukraine as Contributing Partner on March 4, 2022. Minister of Defense of Estonia stated: "Estonia as a Host Nation of the CCDCOE has been a long-term partner for Ukraine in enhancing its cyber security capacity and cyber resilience and we welcome the decision of the members of CCDCOE agreeing to Ukraine's membership" (CCDCOE, 2022). Thus, the collaboration with NATO in cyberspace enabled Ukraine to benefit from NATO's security arrangements in cyber defense without being officially a member of NATO.

Conclusion

Due to the developments in the technology sector, public institutions and private enterprises have moved their operations to the cyberspace to perform their services quickly and precisely. However, the vulnerabilities in operating in the cyberspace have increased in terms of security. The vagueness in defining threats and countermeasures enable the adverse groups to find a grey area to threaten the security of the states, disrupting their digital infrastructure. Therefore, the security of cyberspace has evolved into a vital security field.

As the most successful military alliance in the history, NATO's capabilities to deal with cyber threats have risen since 1999 when it first encountered cyberattacks during the Kosovo Intervention. The most striking embodiment of this evolution has been expressed in the Cyber Defense Pledge at the Warsaw Summit in 2016 where cyberspace is defined as another domain of operations besides land, air, and sea. This declaration enables NATO to mobilize its resources in cyberspace at the operational level, strengthening the Alliance's capability to counter cyberattacks. The contribution of the USA to enhance NATO's cyberspace to deter cyberthreats is another important development. NATO has adopted a pro-active stance in cyberspace. Considering that Russia and China have expanded its cyber operations to disrupt

NATO countries' institutions, especially taking advantage of the lack of definitions and measures in cyberspace, NATO's endeavors in this area are prominent.

Security threats in the cyberspace have a global character. In order to deal with them effectively, the adoption of a global approach is necessary. Being aware of this necessity, NATO has extended its partnerships in cyberspace with supranational organizations such as the EU and other non-EU member European countries. It also established global partnerships with other countries across the world to cope with cyber threats. An important dimension of NATO's global partnerships is that these partnerships enable NATO to share its cybersecurity measures and coordinate activities with those countries whose memberships prospects to NATO is low due to political and geographic reasons. For instance, partnerships with Asia-Pacific countries are especially significant to counter the rising Chinese threat in cyberspace. Ukraine and Georgia benefit from NATO's cyber defense capabilities and experiences without being formal members of NATO.

Yet, NATO is composed of 30 states. Each ally is responsible for its own defense. However, NATO coordinates cyber defense activities and provides a platform for coordination among members. Therefore, the cyber defense capability of each member country is key to boost the total defense capability of the Alliance. The close coordination of cyber defense policies and a common understanding in responding to cyber threats are necessary for NATO's evolution as a global cybersecurity organization.

BIBLIOGRAPHY

AAP-06 Edition 2021. (2021). Brussels: NATO Standarization Office.

Arts, Sophie. (2019). "Offense as the New Defense: New Life for NATO's Cyber Policy", The German Marshall Fund of the United States, https://nato-engages.org/wp-content/uploads/2019/04/Offense-as-the-New-Defense-New-Life-for-NATO's-Cyber-Policy.pdf (Date of Accession: 10.04.2022).

Buresh, Donald. L. (2021). "Russian Cyber-Attacks on Estonia, Georgia, and Ukraine, Including Tactics, Techniques, Procedures, and Effects", Journal of Advanced Forensic Sciences, *1*(2), 15–26.

Buzan, Barry. (1987). An Introduction to Strategic Studies. Hampshire and London: The Macmillan Press Ltd.

CCDCOE. (2022). "Ukraine to be accepted as a Contributing Participant to NATO", CCDCOE, https://ccdcoe.org/news/2022/ukraine-to-be-accepted-as-a-contributing-participant-to-nato-ccdcoe/(Date of Accession: 10.04.2022).

Clark, Mason. (2020). Russian Hybrid Warfare. Washington D.C.: Intitute for the Study of War.

Conklin, Audrey. (2022). "Chinese cyberattacks on NATO countries increase 116% since Russia's invasion of Ukraine: study", Fox Business, https://www.foxbusiness.com/technology/chinese-cyberattacks-nato-increase-ukraine (Date of Accession: 10.04.2022).

Cullen, Patrick. J., & Reichborn-Kjennerud, Erik. (2017). Understanding Hybrid Warfare. London: MCDC.

Davis, Susan. (2019). "NATO in the Cyber Age: Strengthening Security & Defence, Stabilizing Deterrence", NATO Parliamentary Assembly, https://www.nato-pa.int/download-file?filename=/sites/default/files/2019-10/REPORT 148 STC 19 E rev. 1 fin - NATO IN THE CYBER AGE.pdf (Date of Accession: 07.04.2022).

Erlanger, Steven, & Shear, Michael D. (2021). "Shifting Focus, NATO Views China as a Global Security Challenge", *The New York Times*, 14 June. https://www.nytimes.com/2021/06/14/world/europe/biden-nato-china-russia.html (Date of Accession: 11.04.2022).

Fendorf, Kyle, & Miller, Jesse (2022). "Tracking Cyber Operations and Actors in the Russia-Ukraine War", Council on Foreign Relations, https://www.cfr.org/blog/tracking-cyber-operations-and-actors-russia-ukraine-war (Date of Accession: 11.04.2022).

Fortinet. (2016). "NATO Signs Cyber Partnership Agreement With Fortinet", https://www.fortinet.com/corporate/about-us/newsroom/press-releases/2016/nato-signs-cyber-partnership-agreement-fortinet (Date of Accession: 07.04.2022).

Hathaway, Melissa E., & Klimburg, Alexander. (2012). "Preliminary Considerations: On National Cyber Security", Alexander Klimburg (Ed.), National Cyber Security Framework Manual (pp. 1–44). Brussels: NATO CCD COE Publications.

Healey, Jason. (2011). "Cyber Attacks Against NATO, Then and Now", Atlantic Council, https://www.atlanticcouncil.org/blogs/new-atlanticist/cyber-attacks-against-nato-then-and-now/ (Date of Accession: 06.04.2022).

Herzog, Stephen. (2011). "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses", Journal of Strategic Security, *4*(2), 49–60.

INTERPOL. (n.d.). "Cybercrime", https://www.interpol.int/content/download/5267/file/Cybercrime.pdf (Date of Accession: 06.04.2022).

Mancuso, Mario, Mullick, Sanjay, & Iloulian, Jeremy. (2021). "Cyber Threats from North Korea and China: Risks and Recommendations", The Review of Banking & Financial Services, *37*(3), 31–41.

NATO. (n.d.) "Cyber Coalition", https://www.act.nato.int/cyber-coalition (Date of Accession: 07.04.2022).

NATO. (2011a). "Defending the networks The NATO Policy on Cyber Defence", https://www.nato.int/nato_static/assets/pdf/pdf_2011_08/20110819_110819-policy-

cyberdefence.pdf (Date of Accession: 07.04.2022).

NATO. (2011b). "Cyber defence: next steps", https://www.nato.int/cps/en/SID-867C8DF7-C161CCEB/natolive/news_75358.htm (Date of Accession: 07.04.2022).

NATO. (2016a). "NATO Cyber Defence", https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160627_1607-factsheet-cyber-defence-en.pdf (Date of Accession: 07.04.2022).

NATO. (2016b). "Cyber Defence Pledge", https://www.nato.int/cps/en/natohq/official_texts_133177.htm (Date of Accession: 07.04.2022).

NATO. (2018). "Brussels Summit Declaration", https://www.nato.int/cps/en/natohq/official_texts_156624.htm (Date of Accession: 07.04.2022).

NATO. (2021a). "Brussels Summit Communiqué", https://www.nato.int/cps/en/natohq/news_185000.htm (Date of Accession: 07.04.2022).

NATO. (2021b). "NATO Cyber Defence", https://www.nato.int/nato_static_fl2014/assets/pdf/2021/4/pdf/2104-factsheet-cyber-defence-en.pdf (Date of Accession: 07.04.2022).

NATO. (2021c). "NATO 2030", https://www.nato.int/nato_static_fl2014/assets/pdf/2021/6/pdf/2106-factsheet-nato2030-en.pdf (Date of Accession: 07.04.2022).

NATO. (2021d). "Relations with partners across the globe", https://www.nato.int/cps/en/natohq/topics_49188.htm (Date of Accession: 07.04.2022).

NATO. (2022). "Cyber defence", https://www.nato.int/cps/en/natohq/topics_78170.htm (Date of Accession: 07.04.2022).

NATO Parliamentary Assembly. (2021). "NATO PA President's statement on the attribution of large-scale cyber hacks to China", https://www.nato-pa.int/news/nato-pa-presidents-statement-attribution-large-scale-cyber-hacks-china (Date of Accession: 07.04.2022).

NATO StratCom. (n.d.). "2007 cyber attacks on Estonia", https://stratcomcoe.org/cuploads/pfiles/cyber_attacks_estonia.pdf (Date of Accession: 07.04.2022).

NCI Agency. (n.d.) "Multinational Cyber Defence Capability Development (MN CD2)", https://www.ncia.nato.int/what-we-do/cyber-security/multinational-cyber-defence-capability-development.html (Date of Accession: 07.04.2022).

NCI Agency. (2018). "NATO to sign new cyber partnerships with Industry in Berlin", https://www.ncia.nato.int/about-us/newsroom/nato-to-sign-new-cyber-partnerships-with-industry-in-berlin.html(Date of Accession: 07.04.2022).

NCIP. (n.d.). "Our objectives and principles", https://nicp.nato.int/objectives-and-principles/index.html (Date of Accession: 07.04.2022).

Nocetti, Julien. (2018). "Cyber Power", Andrei. P. Tsygankov (Ed.), Routledge Handbook of Russian Foreign Policy (pp. 182–199). New York: Routledge.

Pearson, James & Landay, Jonathan (2022). "Cyberattack on NATO could trigger collective defence clause - official", Reuters, https://www.reuters.com/world/europe/cyberattack-nato-could-trigger-collective-defence-clause-official-2022-02-28/ (Date of Accession: 07.04.2022).

Savage, Olivia. (2022). "NATO refreshes cyber technology, competition to replace equipment under way", Janes. https://www.janes.com/defence-news/news-detail/nato-refreshes-cyber-technology-competition-to-replace-equipment-under-way (Date of Accession: 07.04.2022).

Schmidt, Michael N. (Ed.). (2005). Tallinn Manual on the International Law applicable to cyber warfare. Cambridge University Press. https://issuu.com/nato_ccd_coe/docs/tallinnmanual (Date of Accession: 02.04.2022).

Siman, Bernard. (2022). "Hybrid Warfare Is Not Synonymous with Cyber: The Threat of Influence Operations", Security Policy Brief, *155*, 1–4.

Theiler, Olaf (2011). "New threats: the cyber-dimension", NATO Review, https://www.nato.int/docu/review/articles/2011/09/04/new-threats-the-cyber-dimension/index.html (Date of Accession: 07.04.2022).

The Guardian. (2007, May 17). "Russia accused of unleashing cyberwar to disable Estonia", https://www.theguardian.com/world/2007/may/17/topstories3.russia (Date of Accession: 10.04.2022).

The International Telecommunication Union. (n.d.). "Introduction to Security Cyberspace, Cybercrime and Cybersecurity", https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Introduction to the Concept of IT Security.pdf (Date of Accession: 02.04.2022).

United Nations Office on Drugs and Crime. (2010). "Cybercrime", https://www.unodc.org/documents/data-and-analysis/tocta/10.Cybercrime.pdf (Date of Accession: 02.04.2022).

U.S. Department of Defense. (n.d). "Cyberspace Operations Lexicon", https://info.publicintelligence.net/DoD-JointCyberTerms.pdf (Date of Accession: 02.04.2022).

Wilson, Clay. (2008). Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress. Washington D.C.: Congressional Research Service.