DOI: 10.53477/2668-2001-21-18

NATO'S ENCOUNTERS IN THE CYBER DOMAIN

Dragoș-Mihai Păunescu[1]
"Carol I" National Defence University

Abstract

Last two decades technological advances in artificial intelligence, autonomous systems, telecommunications or space assets, brought new threats for the international security and have fundamentally changed the nature of warfare. Coercive cyber aggressions between opponents have enough potential to affect the digital economy and national security services without escalate into traditional conflicts. Cyber threats to Western security organizations are becoming more frequent, complex, and destructive. NATO's strategic competitors such as Russia and China seek to shape cyberspace through state action in order to gain an asymmetric military advantage. By adapting its posture in the cyber domain, refining doctrine and developing new capabilities, NATO aims to deter cyber aggressions against its interest and to coordinate better the defense of its member states.

Keywords: cyber security; cyber warfare; defense concepts; NATO; Russia; China.

INTRODUCTION

Since the end of the Cold War, radical groups, terrorist organizations together with intelligence agencies and military regimes that controlled weapons of mass destruction, represented the most plausible world's threats. In the last two decades, the security environment witnessed a significant shift: the world's most relevant state actors shifted the focus from being nuclear powers competing in an arms race to becoming cyber powers that allows much softer tools to be employed to achieve military objectives.

Nowadays increasing connectivity and reliance on information technology is a vulnerability recognized by NATO and national security doctrine as it is being targeted by cyber-attacks and subversion of democratic institutions carried out by disinformation.

Just as in the traditional domains, cyber threats for NATO are emerging from a wide range of sources that include state actors, especially China and Russia, but also a significant number of non-state actors, including proxies and criminal organizations. Cyber operations performed by opposite actors are likely to target NATO Computer & Information Systems (CIS) infrastructure and data bases to affect the communications' confidentiality, reliability or availability either in reality or in perception.

Due to the interconnected and omnipresent nature of cyberspace and the fact that cyber operations are cheap, accessible, discreet, stealthy and have the element of plausible deniability, they can result in disproportionate effects against a technology-dependent organization or even nation.

INCREASING CYBERSPACE CHALLENGES

Russia represents a significant cyber threat to NATO and this has already been demonstrated by integrating cyber in the operations carried out during the Georgia and Ukraine/Crimea conflicts. Cyber is a low cost and deniable tool, especially when "*non-state*" proxies are used. The use of Moscow proxies to disrupt and destabilize the civilian population and critical infrastructure particularly in its near abroad, but also in NATO/EU space bordering Russian territory, is a distinct possibility.

Generally, a proxy is in the service of a state-actor when the respective state lacks the required skills, knowledge and means to operate in cyberspace. Another important reason for state actors to use proxies could be associated to political unwillingness to openly employ state resources, especially in those cyber operations that contradict legal, ethical, cultural or assumed norms. A state

[1] Corresponding author: Dragos.paunescu@lc.nato.int

operating through proxies could demonstrate plausible deniability, whilst not exposing state-owned technical capability.

Often Moscow has an important influence on elections, public opinion and even politicians using information warfare and cyber-attacks. Russian also interfered with NATO exercises and other Baseline Activities and Current Operations (BACO) using cyber operations, but also Electronic Warfare (EW) interference (including GPS jamming) to disrupt Alliance's events. To estimate the impact and the effectiveness of such activity coordinated by Moscow is difficult given the challenges faced by NATO and its members individually to implement effective cyber defense capabilities.

Cyberspace consists mostly of artificially constructed computerised environment that is global and interconnected, but which is restricted by jurisdiction national and international barriers. Even if NATO affirmed that international law applies in cyberspace (Wales Summit Declaration 2014), for many other actors, including state ones, anything that cannot be punished for or retaliated against is allowed.

Cyberspace was considered an enabling element for the three traditional domains, but military is now relying more and more on secured access to cyber as a perquisite for the deployment and activation of forces and has been granted to cyber the domain relevance. Cyber domain is part of NATO's collective defense commitment as the other traditional domains confirmed by member states official position and by NATO Secretary General statement that "*A serious cyberattack could trigger Article 5*" (https://www.nato.int 2019).

During the COVID-19 pandemic, the need for more security in the digital world has heightened. Because of the increased online presence, requested to preserve human social and professional relations, new opportunities emerged for cybercriminals who targeted the online commerce and financial tools, as well as the healthcare system.

The EU High Representative Josep Borrell, in April and the NAC, on 3 June 2020, condemned the destabilizing and malicious cyber activities performed in the context of the coronavirus pandemic (Statement by the North Atlantic Council concerning malicious cyber activities 2020). NATO statement expressed the solidarity and mutual support for those affected by malicious cyber activities, including healthcare services, hospitals and research institutes. The statement also requested the respect for international law and norms of responsible state behavior in cyberspace after disinformation campaigns conducted from China or Russia flooded Western media and social networks.

The limited military cyberspace resources have to be employed carefully, only in the necessary areas otherwise the Internet could easily absorb entire cyber capabilities. The military activities have to remain limited in the cyberspace, targeting only specific areas of interests. The largest part of cyber activities is performed and controlled by private entities in both EU and US, and all allied operations and missions have some degree of reliance on civilian government or private industry, mainly in the field of communications infrastructure, logistics, equipment, or host nation critical national infrastructure.

Alexander Glenn, senior research for NATO and Cyber policy, identified four major cyberspace activities related to the military: intelligence, information, crime and military operations: "*militaries participate in intelligence operations, conduct information operations, conduct and support conventional and special operations, and respond to a limited subset of crime. Together these four areas make up the military cyber domain* (Crowther 2017)."

ADAPTING THE ALLIANCE'S CYBER POSTURE

Facing new complex and destructive threats coming from the cyber environment, NATO has to adapt its doctrine and structures to the evolving security landscape. The need to enhance NATO's collective defense capabilities, in order to be able to respond to the cyber threats, was first agreed by the decision makers during 2002 NATO summit meeting in Prague. Starting this point, the subject's relevance constantly increased, receiving central emphasis on the Alliance's meeting's agenda. After in 2008 a dedicated defense policy was approved, in 2014 cyber defense became part of collective

defence, allies admitting that cyber-attacks could trigger the activation of Alliance's founding treaty Article 5.

Because of the technological evolution, NATO's traditional operating environments have been supplemented and the Alliance declared that cyber is a "*domain*" of military operations, similar to air, land, and sea domains[2] and endorsed the development of national cyber defense infrastructure as a priority. While "*domain*" is defined by Merriam-Webster as a sphere of knowledge, influence, or activity , cyberspace is defined by AJP-3.20, Allied Joint Doctrine for Cyberspace as: "*The global domain consisting of all interconnected communication, information technology and other electronic systems, networks and their data, including those which are separated or independent, which process, store or transmit data*."[3] The Alliance's purpose regarding cyberspace was clarified by the declaration issued after the NAC meeting in Brussels during the NATO summit 2018: "*We must be able to operate as effectively in cyberspace as we do in the air, on land, and at sea to strengthen and support the Alliance's overall deterrence and defense posture*." (Brussels Summit Declaration 2018) During the Brussels Summit NATO's members expressed their determination *"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* ", as a major step for including the cyber-attacks in the threshold Article 5 collective defense commitment.

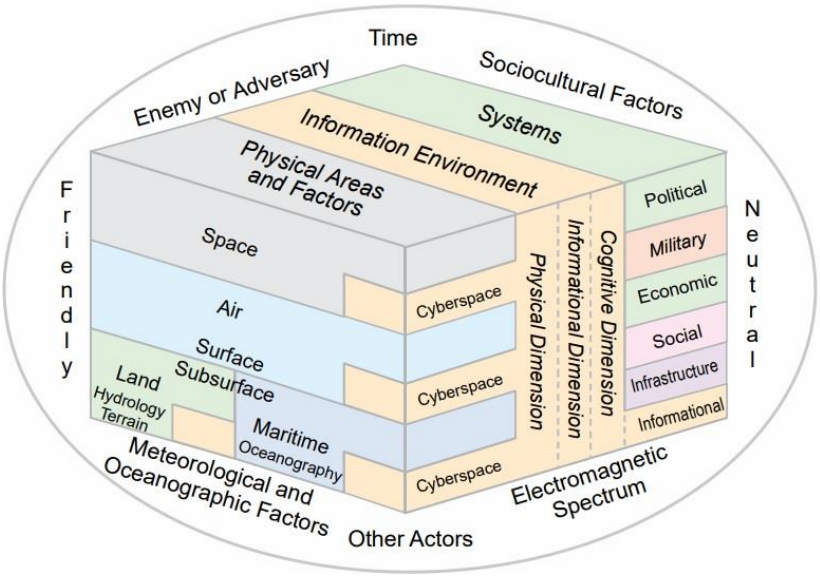

Figure 1. Holistic view of the Operational Environment

Joint Publication 5-0, Joint Planning, released on December 1st, 2020, offers the diagram above as example of the Operational Environment, comprised of the stated domains: Land, Air, Maritime, Space, and Cyberspace.

Each domain has specific characteristics that implies different ways to conduct operations, to create desired effects and furthermore, to achieve decisive conditions and objectives in the operational environment. Through cyber operation, a wide range of effect can be generated either in cyberspace or in other domains and environments by both friendly and opposite entities.

In July 2016, Allies reaffirmed NATO's defensive mandate and recognized cyberspace as a domain of operations. As a consequence, the Alliance's adaptation process had to focus to enhance the resilience of capabilities and assets, to coordinate and deconflict resourcing priorities during

[2] US Department of Defense (DoD) and later NATO recognized "space" also as a domain of military operations.
[3] DoD define cyberspace as "A global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers".

NATO planning of operations. Cyberspace operations are integral part of Alliance operations and missions and have to be considered since the early stages of planning.

To counter cyber threats is complex due to the fact that significant amount of actions could happen below the threshold of armed conflict, fact presented by the US Cyber Command, which recognized that "*adversaries operate continuously below the threshold of armed conflict to weaken institutions and gain strategic advantages*. (Achieve and Maintain Cyberspace Superiority 2018)".

NATO is assisting its member and partner nations in the cyberspace domain by sharing information and best practices, and by conducting cyber defense exercises to help develop national expertise. NATO established at its level a multinational and interdisciplinary cyber defense hub, the Cooperative Cyber Defense Centre of Excellence in Tallinn-Estonia, which mission is "*to support our member nations and NATO with unique interdisciplinary expertise in the field of cyber defense research, training and exercises covering the focus areas of technology, strategy and law"* (NATO Cooperative Cyber Defence Centre of Excellence n.d.).

In October 2018, the Alliance declared the initial stand up of the Cyberspace Operations Centre, (CyOC) in Mons-Belgium, that functions at the strategic level as part of NATO's strengthened Command Structure. The CyOC serves as NATO's theatre component for cyberspace and has the mission to provide cyber situational awareness (SA), to synchronies the related planning aspects and to coordinate operational activity in cyberspace, ensuring freedom to act in this domain and enhancing the Alliance's resilience. This center, that is to be fully operational in 2023, represents the most significant NATO Command Structure Adaptation (NCS-A) measure for the cyber domain and make use of national cyber capabilities for its missions and operations.

Figure 2. CyOC position in NATO Command Structure. (Portuguese Military Academy - NATO Cyber Defence n.d.)

Other allied cyber capabilities are based in SHAPE, in Mons, like the NATO Computer Incident Response Capability (NCIRC), which protects the Alliance's networks by rapidly providing centralized cyber defense support, or the NATO Cyber Rapid Reaction teams that are on standby to assist NATO members, 24 hours a day, if requested and approved.

To facilitate capability development under a NATO-wide and common approach cyber defense, the alliance defines targets for member countries' implementation of national cyber capabilities using the NATO Defense Planning Process.

Following Bucharest's determination to improve cyberspace regulatory framework and to integrate cyber effects in joint operations, starting December 2018, Romania also established a strategic-operational military cyber-agency, the Cyber Command. The agency's mission is to plan, synchronize and conduct cyber activities in order to protect and increase the resilience of CIS infrastructure that supports military operations. (The Cyber Command n.d.)

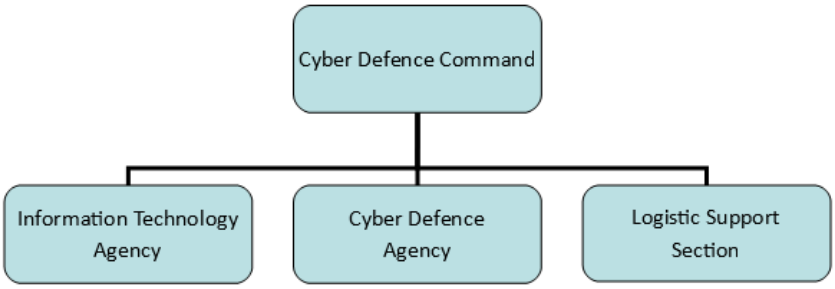

Figure 3. Romanian Cyber Defense Command Structure

In addition to NATO organizational adaptation, members agreed at the Brussels Summit on how to integrate sovereign cyber effects, provided voluntarily by nations, into the Alliance's operations and missions. Allies established mechanisms to enhance information-sharing and mutual assistance in preventing, mitigating and recovering from cyber-attacks.

NATO is cooperating with the EU through a Technical Arrangement on Cyber Defense, signed in February 2016, which allows both organizations to exchange information related to cyber-defense. The agreement involved both organizations specialized structures, NCIRC and the Computer Emergency Response Team – European Union (CERT-EU) and granted access for EU staff members to NATO exercises "*Cyber Coalition*" (Cybersecurity in the EU Common Security and Defence Policy, Challenges and risks for the EU 2017). Up to that time, at the EU level, in order to mitigate cyber threats to its security, the European Union Agency for Cybersecurity (ENISA), an agency dedicated to achieving a high common level of cybersecurity across the union, had been established in 2004. According to its mission statement, ENISA "*contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow*" (ENISA – The European Union Agency for Cybersecurity n.d.). Having common challenges, NATO and the EU are further consolidating their cooperation on cyber defense, particularly on information exchange, research, training and exercises.

CONCLUSIONS

NATO's potential adversaries are developing offensive cyber capabilities to exploit ridges and vulnerabilities in order to confuse and undermine the Alliance's reaction in future conflicts. The constant technological adaptation of the NATO and national security forces to the current strategic scenarios is essential to maintain a reliable defense posture.

The EU and NATO are targeted by similar cybersecurity threats that undermine, in various degrees, all operational environment factors, political, military, economic, social, information, infrastructure, and their cooperation is leading to common or complementary defense solutions.

By constantly adapting its structure and posture, NATO is able to face new emerging threats and to increase its reediness and responsiveness in all operational domains. The Alliance's adaptation process comprise also the development of policies and capabilities for the cyber domain designated to improve the understanding of different threats and risks and its ability to react in order to achieve NATO's ambitions for the cyberspace.

Given that, over the past few years, the frequency and complexity of the cyber-attacks and their potential to generate instability grew substantially, the need to achieve consensus for a an worldwide recognized legal framework in the cyber domain should become a high priority for international organizations.

REFERENCES

Achieve and Maintain Cyberspace Superiority. US Cyber Command, 2018.

Brussels Summit Declaration. July 11, 2018. https://www.nato.int/cps/en/natohq/official_texts_156624.htm?selectedLocale=uk. (accessed November 18, 2020).

Crowther, Glenn Alexander. 2017. "The Cyber Domain". *The Cyber Defence review*: 63-78.

Cybersecurity in the EU Common Security and Defence Policy, Challenges and risks for the EU. 2017. Brussels: European Parliamentary Research Service.

ENISA – The European Union Agency for Cybersecurity. n.d. https://www.enisa.europa.eu/about-enisa (accessed October 17, 2020).

NATO Cooperative Cyber Defence Centre of Excellence. n.d. https://ccdcoe.org/about-us/. (accessed September 09, 2020).

NATO will defend itself. August 27, 2019. https://www.nato.int/cps/en/natohq/news_168435.htm?selectedLocale=en (accessed January 16, 2021).

Portuguese Military Academy – NATO Cyber Defence. n.d. https://academiamilitar.pt/images/site_images/5th_NATO_Cyber_Defence/8_Brigadier_General_HUN_Army_Sandor_VASS_Director_Cyberspace_Operations_Centre_ACO_-_CyOC.pdf,%20accessed%20on%20February%2020,%202021 (accessed February 20, 2021).

Statement by the North Atlantic Council concerning malicious cyber activities. June 03, 2020. https://www.nato.int/cps/en/natohq/official_texts_176136.htm?selectedLocale=en (accessed October 17, 2020).

The Cyber Command. n.d. https://www.cybercommand.ro/pages/view/81 (accessed October 29, 2020).

Wales Summit Declaration. NATO, 2014.