THE EVOLUTION OF NATO'S CYBER SECURITY POLICY AND FUTURE PROSPECTS

Arif Hasan HASANOV *
Khayal Ibrahim ISKANDAROV *
Sadi Saleh SADIYEV *
*War College of the Armed Forces, Republic of Azerbaijan

Abstract: *While the future landscape of cyberspace is becoming quite complicated, NATO must define the potential threats and adapt its strategy to these challenges. In order to form an effective cyber security strategy, a significant number of challenges need to be taken into account for the foreseeable future. Apart from its member states NATO needs to cooperate with significant number of partner nations in order to establish an effective response mechanism against potential cyber threats for maintaining a safe, secure and resilient cyberspace. The paper focuses on the reasons that necessitated the formulation of NATO's cyber security strategy. The evolution of NATO's cyber security policy has been delineated, various aspects of the latest strategy to prevent emerging cyber threats in the modern era and the prospects for partner countries have been examined, the proposals have been put forward to improve the cyber capabilities of Azerbaiajn Republic in cooperation with NATO. The paper seeks the best crisis response strategy which most effectively integrates the respective strengths and capabilities of both member and partner nations. Through only this strategy greater resilience when dealing with threats can be achieved.*

Key words: cyber security, cyber defence, cyber threat, cyberspace, cooperation

1. INTRODUCTION

Cyberspace is an integral part of the security environment and plays a decisive role in improving the operations' capabilities. With the development of the internet cyber security has become a central topic for international security.

A cyber-attack is "the premeditated use of disruptive activities, or the threat thereof, against computers or networks, with the intention to cause harm or to social, ideological, religious, political or similar objectives or

intimidate any person in furtherance of such objectives" [1]. Cyber warfare refers to all state actions that make use of internet and aim at damaging opponents.

Cyber security, in short, has become a crucial component of national and economic security strategy, has quickly evolved from a technical discipline to a strategic concept. The challenges the Alliance faces are changing in fundamental ways.

The old threat scenario involving direct intervention has been replaced by the challenge posed by invisible adversaries whose geographical source can often not be determined [2]. For Hansen and Nissenbaum, cyber security is "a concept that arrived on the post-Cold War agenda in response to a mixture of technological innovations and changing geopolitical conditions" [3].

The real world examples prove that the ubiquity and vulnerability of the Internet have tangible political and military ramifications. Some cyber-attacks could have the same level of disruption on the countries and economies as conventional warfare. As Cetron and Davies observe "major concern is no longer weapons of mass destruction, but weapons of mass disruption" [1].

2. THE EVOLUTION OF NATO'S CYBER SECURITY POLICY

Cyber security is an area in constant flux – the work will never be completed. Cyber is a domain that affects both the civil and military division. As cyber threats evolve and pose severe challenges to states, companies and individuals on a daily basis, it is vital that actors such as NATO continue to work closely, and strive to establish new and effective ways to protect cyberspace [4].

NATO suffered its first cyber-attacks in 1999, when hackers blocked access to the organization's websites and e-mail servers to protest the air strikes against Serbia. These protest attacks were conducted by Russian, Serbian, and Chinese hackers. Then NATO Computer Incident Response Capability (NCIRC) was created which was the Alliance's "first responders" to prevent, detect, and respond to cyber incidents [5].

One of the first and most powerful political move worldwide in this field was brought about by

the United States of America (USA) in the aftermath of the September 2001 terrorists attacks with the formulation of its National Strategy to Secure Cyberspace [3].

Since the early 2000's NATO, as a defense alliance, has been aware of cyber threats and the importance of protecting vital and critical information infrastructure networks [6]. In November 2003, nine NATO nations (Canada, France, Germany, Italy, Netherlands, Norway, Spain, UK and US) signed an arrangement to share more information about cyber security. Later, in the same year, NATO approved the Cyber Defense Programme and Computer Incident Response Capability to prevent, detect and respond to cyber threats.

Even though NATO had eight years after Serbian cyber-attacks to prepare, yet in 2007 it failed to prevent cyber-attacks in Estonia. Following the cyber-attacks against Estonia's public and private institutions, Allied defense ministers agreed in June 2007 that urgent work was needed in this area. As a result, NATO approved its first Policy on Cyber Defense in January 2008.

In the summer of 2008, the conflict between Russia and Georgia demonstrated that cyber-attacks had the potential to become a major component of conventional warfare [7]. One year after the cyber-attack on Estonia a similar to the scenario played out in Georgia. Vulnerabilities in the information infrastructure of the Georgian Government were detected by hackers through the Distributed Denial of Service method and Georgia was exposed to heavy attacks. These cyber-attacks were organized not only from Russia but also from various other regions in the world.

NATO could not provide direct assistance to Georgia, since it was not a member state of the alliance. However, due to increased attacks, a group of subject matter experts was sent to Georgia on the initiative of Estonian government. With the support of these experts, information system in the country were normalized shortly after the prolonged cyber-attacks [8].

The 2008 Bucharest Summit emphasized "the need for NATO and nations to protect key information systems; to share best practices and to provide a capability to assist Allied nations, upon request, to counter a cyber-attack" [5].

In March 2009, a network of compromised computers attacked

the computer systems of government and private organizations in over 100 countries, accessing sensitive and confidential documents [9].

In May 2009, President Obama made a dramatic announcement: "Cyber intruders have probed our electrical grid ... in other countries, cyber-attacks have plunged entire cities into darkness." Investigative journalists subsequently concluded that these attacks took place in Brazil, affecting millions of civilians in 2005 and 2007, and that the source of the attacks is still unknown. National security planners should consider that electricity has no substitute, and all other infrastructures, including computer networks, depend on it [2].

NATO's latest Strategic Concept underscores that cyber threats constitute direct challenges to national critical infrastructures and that they may reach levels such as "to threaten national and Euro Atlantic prosperity, security and stability". Therefore, they require NATO to develop its ability to prevent, detect and defend against these threats, recover after cyber-attacks and enhance and coordinate national cyber defense capabilities [6].

On June 8, 2011, NATO Defense Ministers adopted a new cyber defense policy. The policy focused on prevention of cyber-attacks and building resilience. The creation of the Rapid Reaction Team was a result of the Alliance's revised cyber defence policy of 2011.

The main elements of the new approach included [5]:

1. Realization that cyber defense is required to perform NATO's core tasks of collective defense and crisis management;
2. Prevention, resilience, and defense of cyber assets critical to NATO and its constituent Allies;
3. Implementation of robust cyber defense capabilities and centralized protection of NATO's own networks;
4. Definition of minimum requirements for cyber defense of national networks critical to NATO's core tasks;
5. Assistance to the Allies to achieve a minimum level of cyber defense to reduce vulnerabilities of national critical infrastructure;
6. Engagement with partners, other international organizations, the private sector, and academia.

At the 2011 Munich Security Conference, then-German Minister of Interior Thomas de Maizière revealed that the German

government network is attacked four to five times a day by foreign intelligence services [9].

In 2012 at the Chicago Summit, it was realized that there were still important coordination failures among the member states. For this reason, in 2013, five NATO member states [Denmark, Holland, Canada, Norway and Romania] initiated Multinational Cyber Defense Capability Development Project for further cooperation and coordination. However, this project was not very efficient as it was supported only by these five countries [8].

To keep pace with the rapidly changing threat landscape and maintain a robust cyber defense, NATO adopted an enhanced policy and action plan, which was endorsed by Allies at the Wales Summit in September 2014. The policy establishes that cyber defense is part of the Alliance's core task of collective defense [7]. This means that the NATO will respond with conventional weapons in case of a severe cyber-attack confirming that the Internet is a new battlefield [6].

Now Article 5 of the North Atlantic treaty requires member states to come to the aid of any member state subject to an armed attack, which includes cyber-attack in the new cyber defense policy. Official recognition of cyberspace as a domain of warfare means that, under Article 3 of the Washington Treaty, that member states have a responsibility to defend and develop national cyber security infrastructure in order to [10]. Designating cyberspace as an operational domain means that the NATO will spend a significant effort in improving cyber capabilities of its members, it is expected more focus on training and military planning. The cyber defense of the alliance will continue to be integrated into operational planning and its operations and missions

To enhance situational awareness, a Memorandum of Understanding on Cyber Defense was developed in 2015. It sets out arrangements for the exchange of a variety of cyber defense-related information and assistance to improve cyber incident prevention, resilience and response capabilities [7].

At the Warsaw Summit in 2016 member states made significant long-term decisions on cyber security, including recognition of cyber space as a fifth domain of warfare, in which will be operational, in addition to air, sea, land and space [10]. "Now, in

Warsaw, we reaffirm NATO's defensive mandate, and recognize cyberspace as a domain of operations in which NATO must defend itself as effectively as it does in the air, on land, and at sea. This will improve NATO's ability to protect and conduct operations across these domains and maintain our freedom of action and decision, in all circumstances" states the Warsaw Summit Communiqué [11].

On 16 February 2017, defense ministers approved an updated Cyber Defense Plan as well as a roadmap to implement cyberspace as an operational domain. This will increase Allies' ability to work together, develop capabilities and share information [7].

At the Brussels Summit in 2018, Allied leaders agreed to set up a new Cyberspace Operations Centre as part of NATO's strengthened Command Structure. The Centre will provide situational awareness and coordination of NATO operational activity within cyberspace. Allies also agreed that NATO can draw on national cyber capabilities for its missions and operations. Finally, Allies took stock of their progress to enhance national resilience through the Cyber Defence Pledge [7].

3. LESSONS LEARNED AND THE PROSPECTS OF FURTHER COOPERATION

When it comes to cyber security, NATO has come a long way. It can broadly be divided into three stages: the first one was when cyber security was treated more as a technical challenge which was supposed to be faced separately by the Atlantic Alliance and its institutions in relation to the ICT infrastructure used by NATO, and separately by the member states with regard to their national ICT networks; the second one was when the topic became an important political issue (the process was primarily initiated during the Riga Summit and subsequently stepped-up following the cyber-attacks against Estonia); and finally the third one when NATO declared cyber security to be a strategic challenge, requiring a coordinated response on the part of the entire Alliance and all Member States, perhaps even under Article 5 of the Washington Treaty (conclusions of the Wales Summit) [12].

There are three dimensions of cyber-attacks:

– attacks that focus on strategic objectives;

– attacks that focus on technical objective;

– attacks of a political nature.

Attacks with a strategic focus those on include information systems, communications, and civil security; technical targets include weapons control and military communications; while political assaults look to alter the power balance within diplomatic relations. Cyber weapons include viruses, malware, denial of service, spying, along with jamming and blocking [1].

The 2007 cyber-attack on Estonia that temporarily crippled Estonia's national internet infrastructure was a wake-up call for NATO. . But this type cyber-attack is actually just one of many threats, and probably not the most damaging one. Another fact is that in the Estonian cyber-attack there was not clear evidence who was responsible. In Georgia the cyber-attack was speculated to be conducted at the behest of another state which is still unclear.

Cyber threats have become more and more serious during the last years. They are not limited by boundaries and have increased in sophistication and frequency. The global ownership over the cyberspace and its potential globalizing effect, as well as the increased security risk represented by cyber-attacks, all show the need to work together in international cooperation towards collective cyber security [13]. Experts estimate that there are hundreds of millions of malicious programs and more than 100 organisations that participate in military, intelligence or cyber terrorist operations [9]. Thus, NATO operations rely heavily on cyber-enabled networks. Cyber threats need to be taken seriously and perceived as a strategic matter, at the same time should not be exaggerated as revolutionary.

In recent years, cyber security has become a high ranking issue threatening stability worldwide. The age of mega-breaches has arrived, cyber security going hand in hand with fighting an almost invisible and unconventional enemy lurking in the shadows of an anarchic cyberspace.

Cybercrimes are increasing because of global interconnectedness, coupled by inadequate protective measures exposing government and private organizations as well as infrastructures to cyber threats. The key solution is of course resilience, the necessity to build smarter and faster ways to detect

attacks and to promptly counter them [14].

Today's cyber threat landscape is markedly different from that of a few years ago. Experts and officials agree that the speed of attacks and their sophistication has changed dramatically. Another vital difference lies in their diversity. Cyber risks threaten the benefits, whether economic, political or social that the human invention of cyberspace can offer. Many more states now consider cyber capabilities as a legitimate and necessary part of their strategic toolbox alongside diplomacy, economic prowess and military might [15].

NATO has made considerable progress in its efforts to integrate cyber security into its planning processes, but according to James Lewis, while it may have gone as far as the political environment allows it needs to done more. For example, a report by the defense committee of the UK parliament finds that NATO is poorly prepared to respond to Russia's possible use of asymmetric warfare, including cyber-attacks, information and psychological operations. The committee urges the alliance to develop its own asymmetrical warfare capabilities, discuss how to deal with these attacks and operations and mount its own offensive operations [6].

Everything indicates that in the coming years, the discussions on the direction of the Alliance's involvement in cyber operations will be dominated by two issues. The first one concerns the need for the Alliance to specify exactly the activities carried out in the framework of collective defense and the development of NATO's capabilities, also offensive, to operate in cyberspace. The second one, which is frequently brought up in the discussion about the cyber security of the Alliance, is the need for comprehensive measures to be implemented to counter hybrid threats, including the multi-dimensional use of cyberspace as one of the most critical elements [12].

Nonetheless, academics such as Thomas Rid are of the view that cyber war will not take place. Experience to date on the actual uses of cyber capabilities by states suggests such capabilities are better characterized as either espionage or sabotage, making their employment most likely below the threshold of armed attack. While there is a certain logic to this argument, it is increasingly clear that some states

consider cyber capabilities as an integral part of operational military capability and are not afraid to employ them as such, even if they are reluctant to acknowledge such use publicly [15].

In cyber conflict, the terrestrial distance between adversaries can be irrelevant because everyone is a next-door neighbour in cyberspace. And of course it necessitate cooperating internationally. As Jamie Shea, NATO deputy assistant secretary general for emerging security challenges mentioned: NATO has agreed a series of actions that can be taken in the form of assistance to allies, he said, including training, education, exercises, malware intelligence sharing, early warning, and incident response. The third key element of the enhanced NATO cyber defense policy is multi-national cooperation in cyber defense, which includes the concept of "smart defense" through pooling and sharing capabilities. This means that all future NATO military exercises will involve a cyber-component and look at the challenges of running military operations in a degraded cyber operating environment [16].

Even though the cyber security is a part of NATO's collective defense, there are some setbacks. According to Salih Bicakci, there are three main reasons of why NATO is still not sufficient on collective cyber security. The first reason is that the capacities of member states on cyber security are different. The second reason is that the threats on cyberspace frequently transform themselves, so adoption process is not easy for everyone. The third reason is that most of the threats come from the private sector, so it is not easy to communicate with the all private sectors in each member state.

According to Piret Pernik, the most important lack of NATO's cyber security policy is the lack of sharing experiences. He argues that more advanced member states, having heavily invested into national cyber capabilities, hesitate sharing these with others for financial and security reasons [6].

As the cyber security expert, Jarno Limnell, has noted, the central barrier to greater cooperation and overall increased cyber capability for NATO has essentially been a certain lack of trust. More powerful allies don't yet fully trust less capable ones with information and knowledge about their abilities and weaknesses and prefer to have bilateral or smaller-scale

multilateral cooperation in the cyber defense domain [17].

Although the allies are able to invoke the Article 5 of the North Atlantic Treaty in case of a cyber-attack, what threshold collective defense will be triggered, and how this threshold will be measured, remains secret as a form of deterrent. "We are keeping that ambiguous so a potential aggressor does not get the idea they can carry out cyber-attacks up to a certain level with impunity," said Jamie Shea, NATO deputy assistant secretary general for emerging security challenges [16].

Piret Pernik argues that, NATO nations need to think about what the criteria are when a cyber-attack qualifies as equivalent to an armed attack, what the strategic implications of such an attack are, what circumstances obligate a collective response (for example does damage to or disruption of private critical networks resulting in serious effects?), and how the problem of attribution can be solved, among other questions [6].

If the cyber defense is considerable a must after the Warsaw summit, many experts are questioning about offensive cyber capabilities of Alliance. Almost every state is working to improve its offensive cyber capabilities too [11]. NATO conducts regular exercises, such as the annual Cyber Coalition Exercise, and aims to integrate cyber defense elements and considerations into the entire range of Alliance exercises, including the annual Crisis Management Exercise (CMX) [7].

Sorin Ducaru, assistant secretary general for emerging security challenges for NATO described three layers of the enhanced cyber defense policy [18]:

– the recalibration and enhancement of the cyber defense paradigm within NATO;

– reinforcement of capability development and capacity building;

– re-evaluation of partnerships and governance in the area of cyber defense.

Without any doubt, the best avenue is to collectively battle cybercrime and to collaboratively reinforce NATO's resilience to cyber-attacks. It underscores that, while NATO conducts business in cyber defense area, a continued emphasis on involving other actors (organizations, Allies, partner nations, private sectors) is essential. The cooperation with different actors to learn to work together, share information and fully grasp the rapid dynamics of

cyber crises. It is critical for creating bonds between specialists of different countries, improving interoperability and practicing the intricacies of preventing malicious cyber threats. It in turn will build trust and strengthen bonds of NATO partnerships.

Prospective cooperation areas in cyber security are increasing interoperability, sharing strategic and technical information and threat assessments, coordinating responses to cyber crisis and engaging partners into NATO's education, exercises and training activities. In order to to help develop national expertise NATO is helping member countries by sharing information and best practices, and conducting cyber defense exercises. Cyber defense is as much about people as it is about technology.

4. CONCLUSION

The ubiquity of cyber threats highlights the need to work together – a key issue when reviewing NATO's role. It came to the fore as a result of the cyber-attacks plotted against both NATO and partner nations. The cooperation between like-minded states and international organizations is the best way to address many cyber risks. NATO has the capabilities to offer a clear platform for exchanging practice between Allies and partners through a more extensive variety means, including NATO's Defense Planning Process.

Such mechanisms might include operational and technical support and advice regarding cyber-defense capability development and implementation. It might entail advice on the establishment of a cyber-security strategy or brokering the exchange of lessons learned and situational awareness on cyber domain.

Even though the cyber-attacks are unlikely to be as lethal as strategic bombs for the foreseeable future, NATO has to brace itself for much more complicated predicaments regarding cyber threats emanating from its rivals. It will take a lot of effort and further bold decisions to move closer towards achieving the goal on thwarting cyber threats before they have important physical ramifications.

If virtual space becomes an inherent part of the NATO operations and exercises it will help the Alliance to adapt to emerging technological challenges. It in turn will necessitate to bridge the gap between Allies. Together

with its member states NATO has to facilitate partner nations' cyber defense capability development and participation in the annual trainings and exercises based on reciprocal interests, shared values and common approaches. There is not any obstacle for partners to cooperate at a technical level. NATO might establish individually-tailored projects in accordance with interests and capacities of partners to enhance their cyber security.

Only when the Allies and trusted partners collectively pursue a cyber-policy, they will be able to successfully prepare themselves for cyber threats to their national security. Even though the cyber defense is a part of collective security, NATO still lacks a stringent deterrence against cyber-attacks.

A stringent deterrence means that a state should have an offensive capability if it is attacked. Thus NATO has to prove that it is not only aware of the gravity of the cyber threat but also ready to defend against it.

REFERENCES

[1] Craig B. Greathouse, "Cyber War and Strategic Thought: Do the Classic Theorists Still Matter?" in *Cyberspace and International Relations: Theory, prospects and challenges* (Springer-Verlag Berlin Heidelberg, November 2014): 21-40, https://bit.ly/2vfnfMp.

[2] Kenneth Geers, *Strategic cyber security* (CCD COE Publication, Tallinn, Estonia, 2011), 9 https://bit.ly/2V9OeYv.

[3] Marion Kokel, *"The Engagement of NATO in Cybersecurity: Securing the 5th Battlefield"* (Universite Libre De Bruxelles, Universite D'europe, Faculte Des Sciences Sociales Et Politiques, 2013-2014), 13, https://bit.ly/2GrZPKb.

[4] Jack Young, *"NATO Warsaw Summit: Cyber Security and The Definition of Cyber as a New Domain"*, Aug. 12, 2016, goo.gl/hKLmWw.

[5] Hac Mehmet Boyraz, *"NATO's cyber security policy"*, goo.gl/gcLS8H.

[6] *"Cyber defence, Romania-NATO"*, last update: December 2014, https://bit.ly/2GoxL9h.

[7] *"Cyber defence"*, last updated: July 16, 2018, https://bit.ly/2Gux6Vd.

[8] Hac Mehmet Boyraz, *"NATO's Cyber Security Policy: The Historical Process and Critical Junctures"*, goo.gl/ncpDpu.

[9] Annegret Bendiek *"European Cyber Security Policy"*, *SWP Research Paper RP*, (October 13, 2012 Berlin), 10, goo.gl/K9Nhzx.
[10] *"NATO's reaffirmed commitment to cyber security"*, August 15, 2016, goo.gl/tdprhtcontent_copy.
[11] Pierluigi Paganini, *"NATO Warsaw summit 2016, what about cyber security?"* July 12, 2016, goo.gl/uaxwWncontent_copy.
[12] *NATO road to cybersecurity*, Kosciuszko Institute's report, July 8, 2016, https://bit.ly/2Xjkc1W.
[13] Jason Healey, Leendert van Bochoven *NATO's Cyber Capabilities: Yesterday, today, and tomorrow*, Atlantic Council, goo.gl/NKGcWC.
[14] Raluca Csernatoni, *"Time to Catch Up: The EU's Cyber Security Strategy"*, March 4 2016, goo.gl/US3kJ2.
[15] *"NATO: changing gear on cyber defence"*, goo.gl/oitkY8.
[16] *"NATO to adopt new cyber defence policy"*, September 03, 2014, goo.gl/tpbcko.
[17] Patrik Maldre, *"Estonia's role in NATO's growing cyber capability"*, September 14, 2016, goo.gl/V1LUXj.
[18] *"NATO's Cyber Defense Mission and Capabilities"*, November 06, 2014, goo.gl/LAjqoy.