Nutsa Nebieridze I Alexander Iatsabidze,
Tbilisi Free University
nnebi20@freeuni.edu.ge I a.latsabidze@freeuni.edu.ge

NORTH ATLANTIC TREATY ORGANIZATION (NATO) AND CYBER SECURITY CHALLENGES

Abstract

The North Atlantic Treaty Organization (NATO), by its nature, has always been aimed at strengthening the security of its members. Accordingly, the defense policy developed by NATO was quite successful in most areas, until it faced a new challenge regarding cyber security. Due to the newness of the field, countries and international organizations are now studying possible ways to deal with cyber threats. Among them, the North Atlantic Treaty Organization has also been trying to develop a successful cyber defense policy since the emergence of this threat. The paper explores the evolution of cyber security and the operation of the North Atlantic Treaty Organization. To better understand each stage of the latter, the large-scale cyberattacks that set the precedent and made future cyber threats from specific countries predictable today, are discussed.

Keywords: Cybersecurity, defense policies, cyberattacks, North Atlantic Treaty Organization (NATO).

Current events in the world have caused a change in NATO's cyber security policy and strategy, more than once. Although the aforementioned has always tried to ensure the protection of its own communication and information systems, the issue of the need for the cyber defense was raised for the first time at the 2002 NATO Prague Summit. Since the main challenge for the world at that time was considered to be terrorism, the member states decided to only collect and share information about cyber threats (Davis, 2019). It can be said that initially the threat was considered less serious, but the situation changed after the 2007 incident. That year, hacktivist groups with close ties to the Russian government, conducted the so-called DdoS (Disruption of denial-of-system)[1] attacks, on Estonian public and private institutions, disrupting their functioning. This is the first case in the world in which cyber actors took down the critical infrastructure websites of a NATO member country, without physical intervention (Herzog, 2011). This event is interesting not only because NATO together with the Estonian government, established the NATO Cooperative Cyber Defense Center[2] in Tallinn, but also because Russian cyber activity became more predictable after studying the specifics of the attack (Oja, 2020). This was reflected in 2008, when Russia again used similar cyber tactics against Georgia and disrupted the function of critically important institutions through DDoS (Andria Gotsiridze, 2019). This event turned out to be a turning point for NATO and the whole world to understand that cyber capabilities could already be used in conventional warfare, which added a new unknown and rather dangerous space to hybrid warfare. Therefore, the Alliance needed to do more than just establish a research center. At the Bucharest Summit in 2008, NATO approved its first cyber defense policy and called on members to look for mechanisms to strengthen cyber defense within their territories (NATO, Bucharest Summit Declaration, 2008).

1 A DDoS attack is carried out on websites and servers by disrupting network services and trying to exhaust application resources. Attackers overload the site with unnecessary operations, causing the website to malfunction or shut down altogether.
2 Cooperative Cyber Defense Center of Excellence (CCDCOE) - this institution is an accredited research and training center of NATO

In 2010, the world witnessed a cyber-attack of an unimaginable scale - Stuxnet[3]. The virus got into the operating network of the Natanzi plant in the Islamic Republic of Iran, via a USB, disabling thousands of centrifuges, and eventually spreading outside the plant. According to researchers, the virus set back Iran's nuclear program by at least two years (Baezner & Robin, 2017). After the 2010 event, in order to improve the security of its members, NATO decided to further refine its approach. As a result, at the 2014 NATO Wales Summit, Allies endorsed a new cyber defense policy that recognized cyber defense as part of NATO's core collective defense mission. This meant that a cyber-attack could trigger Article 5 of the NATO Treaty, underscoring the seriousness of NATO's attitude towards cyber security. In addition, the third article was amended, and the members were instructed to allocate a certain part of their financial resources for cyber defense improvement (NATO, Wales Summit Declaration, 2014). The next stage in the development of NATO's cyber defense policy came in February 2016, at the Warsaw Summit, when the heads of allied states reaffirmed the organization's defense mandate and recognized cyberspace as one of the areas[4] of operations in which NATO should protect itself (NATO, Cyber Defence Pledge, 2016). In addition, NATO and the European Union concluded a technical agreement on cyber defense, to develop an important plan[5] concerning cyber attacks (Stoltenberg, 2016). The above-mentioned fact confirms the importance of the concept of cyber security, to the extent that international organizations have united around it and successfully developed a special plan aimed at cyber defense. In 2021, at the next meeting of NATO member states in Brussels, a new policy was developed in support of three main tasks, according to which NATO should deter, defend and counter the full range of cyber threats at all times - at the political, military and technical levels (NATO, Brussels Summit Communiqué, 2021).

Conclusion

NATO's 2021 cyber defense policy prevented its member states from numerous cyber-attacks and made this issue less relevant. Despite this, the 2022 Russia-Ukraine war brought the relevance of cyber security back to the agenda. At the 2023 Vilnius Summit, the importance of strengthening cyber defense in military, political, technical aspects and the need to cooperate with other international organizations and private companies was emphasized. The member states expressed their desire to establish with their own funds, a virtual support mechanism for cyber incidents - VCISC[6]. VCISC will identify even a minor attack and share information with all members, which is a means of improving and perfecting defense mechanisms (NATO, Vilnius Summit Communiqué, 2023). Consequently, to ensure core missions, collective defense, crisis management and cooperative security, NATO continues to adapt to the changing cyber threat environment and refine its cyber defense policy.

3 Stuxnet was a sophisticated cyberweapon allegedly developed by the US in collaboration with Israel to stop Iran's nuclear program (Fruhlinger, 2022).
4 Cyberspace has been added to land, sea and air space.
5 This technical agreement between NCIRC and the European Union Computer Emergency Response Team (CERT-EU) provides information exchange and sharing of best practices between emergency response teams.
6 Virtual Cyber Incident Support Capability

Bibliography*:*

Andria Gotsiridze, C. S. (2019). *The Cyber Dimension of the 2008 Russia-Georgia War.* Retrieved from Rondeli Foundation: https://gfsis.org.ge/cbgl/blog/view/970

Baezner, M., & Robin, P. (2017). *Stuxnet.* Zürich: Center for Security Studies (CSS), ETH Zürich.

Davis, S. (2019). *NATO IN THE CYBER AGE:STRENGTHENING SECURITY & DEFENCE, STABILISING DETTERENCE.* SCIENCE AND TECHNOLOGY COMMITTEE (STC).

Fruhlinger, J. (2022). *Stuxnet explained: The first known cyberweapon.* Retrieved from CSO: https://www.csoonline.com/article/562691/stuxnet-explained-the-first-known-cyberweapon.html#:~:text=Stuxnet%20is%20a%20powerful%20computer,about%20its%20design%20and%20purpose.

Herzog, S. (2011). Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses. *Journal of Strategic Security*, 49-54.

NATO. (2008, April 3). *Bucharest Summit Declaration.* Retrieved from NATO: https://www.nato.int/cps/en/natolive/official_texts_8443.htm

NATO. (2014, September 5). *Wales Summit Declaration.* Retrieved from NATO: https://www.nato.int/cps/en/natohq/official_texts_112964.htm

NATO. (2016, July 8). *Cyber Defence Pledge.* Retrieved from NATO: https://www.nato.int/cps/en/natohq/official_texts_133177.htm

NATO. (2021, June 14). *Brussels Summit Communiqué.* Retrieved from NATO: https://www.nato.int/cps/en/natohq/news_185000.htm

NATO. (2023, July 11). *Vilnius Summit Communiqué.* Retrieved from NATO: https://www.nato.int/cps/en/natohq/official_texts_217320.htm

Oja, M. (2020). History Education: The Case of Estonia. In M. Oja, *Pedagogy and Educational Sciences in the Post-Soviet Baltic States, 1990–2004: Changes and Challenges* (pp. 143-165). Talinn.

Stoltenberg, J. (2016). *JOINT DECLARATION BY THE PRESIDENT OF THE EUROPEAN COUNCIL THE PRESIDENT OF THE EUROPEAN COMMISSION, AND THE SECRETARY GENERAL OF THE NORTH ATLANTIC TREATY ORGANIZATION.*