„Ante Portas – Security Studies”
2020, No 2(15)
DOI: 10.33674/220202

Thornike ZEDELASHVILI[1]
Georgia

BLACK SEA REGION SECURITY, CYBER WARFARE, AND NEW TECHNOLOGIES

Abstract:
In the wake of technological advances, cyber-attacks are becoming more dangerous, becoming a part of everyday life and an element of all conventional warfare. For Black Sea countries as well as the rest of the world, security is paramount. In discussing the issue, we must analyse the opportunities that the countries of the Black Sea basin have, first of all, the threats posed by Russia. This unpredictable state is carrying out the occupation of territories, military aggression, and large-scale cyber-attacks in this region, which is not a guarantee of peace and security. Russia is trying to influence almost the whole world and especially the Black Sea region – Ukraine, Bulgaria, Romania, Turkey, Georgia with large-scale cyber-hacking attacks and continuous disinformation fake news. Against the background of cyberattacks and misinformation propaganda, it is difficult to determine what kind of safe environment can be created in this region. This requires new research, recommendations, scientific papers, defence strategies. Cooperation with the EU and NATO needs to be strengthened. Following the Warsaw Summit, the Euro-Atlantic Alliance enacted Article 5 of the Washington Treaty, that is, the principle of 'collective defence' in terms of cyber warfare, cyber-attacks, and cyberterrorism. The topic discusses the cybersecurity issues and defence mechanisms of the countries of the Black Sea region, as well as the ongoing processes in the field of cybersecurity in this region. The paper discusses the threats and risks posed by Russia in the field of cybersecurity, as well as its impact on world politics.

[1] Thornike Zedelashvili, PhD student at Caucasus International University, founder of the Internet Publication “Leader”. Email: thomaszedelashvili@gmail.com

Keywords:
Black Sea region, cyberwar, cyberattack, cybersecurity, cyberterrorism, information war, hybrid war, Russian Federation, asymmetric threat, international security

Introduction

Talking about stability and security in the Black Sea region is a very difficult issue today. Let's face it, the invading country dominates the region and does not allow any of its neighbours to act or develop independently. Talking about security would not be complete without considering the context of the EU and NATO, given that the main theme of the paper is the situation created against the background of revolutionary advances in cyber technology when it is difficult to identify the attacker. The Russian phenomenon throughout the world is a noteworthy issue that has great potential and seeks to create a reality that is only in its interests. Russia has almost limitless capabilities not only in the military but also in terms of cybertechnology and information-propaganda, as well as a continuous resource of manipulations, which it carries out continuously. Obtaining facts and evidence is not even an easy task.

The Black Sea region is important for both NATO's European allies and the United States. It is a kind of bridge between East and West. In this region, the interests of Europe, NATO, and the United States often conflict with the interests of Russia. The Kremlin began to assert and consolidate its power in the Black Sea basin against Georgia as early as the 1990s, after the collapse of the Soviet Union, and then consolidated it with the 2008 war, when it launched a powerful cyberattack in parallel with a military offensive. In addition to damaging Georgian government agencies and critical infrastructure, Russia has significantly expanded its occupation. If we analyse the situation with a cold mind it was a rehearsal before the invasion of Ukraine. The military attack on Ukraine in 2014 was accompanied by large-scale cyberattacks, followed by the occupation of territories. The purpose of our article is to determine the defence capabilities of the Black Sea Basin countries in terms of cybersecurity, to present the role of NATO in the Black Sea region, and to assess and analyse cyber threats from Russia. The article uses historical and political research analysis.

Cyberattacks from Russia and Cyber-Defence Capabilities of the Black Sea Region

Cyberwarfare is becoming more visible and dangerous internationally over time than ever before. We can partly agree with the view that cyberwar is a cheaper form of warfare than conventional war. Cyberattacks either precede or accompany all conventional wars.

Russian cyber-aggression extends not only to the countries of the Black Sea basin but also worldwide – both in Europe and in the United States. An example is an attempt to interfere in the 2016 United States presidential election. It is true that despite the completion of the investigation, in this case, it was still not clear, but no one can deny the attempt to intervene. There were also attempts at hacking into elections in Germany, France, and Italy. Russia's cyber-technological advances are so great that it is almost one step ahead of other international actors and does not shy away from indirectly straining relations with NATO. This is not a direct conflict, it is more like a game where elements of the Cold War are abundant – the Kremlin also realizes that the alliance has a military advantage. In this case, a direct attack on any member state or an ally would not be a smart move. At this stage, a form of hybrid warfare is beneficial to Russia – it poses a great threat to NATO member states, but does not cross the red line, the violation of which will lead to the enactment of Article 5 of the Charter. The Kremlin is working innovatively in various conflicts. Due to the specific geopolitical environment, it has successfully managed to adapt cyberattacks to expand its interests. As already mentioned, he continues to occupy countries in the Black Sea region to this day, gradually engaging in hybrid warfare, carrying out disinformation manipulations, and actively using cyber elements. It is interesting what the Russian government's vision is in terms of global threats. In the 2015 version of the Russian National Security Doctrine, the 16th and 17th paragraphs consider the U.S. and NATO as the main adversaries, while the 7th paragraph directly states the role of the Russian Federation in the maintenance of world order[2].

That is, the Russian Federation says that it does not even pose a threat to other countries, but is itself a victim and has the potential to improve to deal with threats from the U.S. and NATO. Of course, it has almost the same approach as the countries of the Black Sea basin. In this

[2] Russian National Security Strategy, *Edict of the Russian Federation President – On the Russia Federation's National Security Strategy*, Moscow 2015, pp. 1-4.

case, sometimes it is in the role of a saviour, sometimes it is in the role of a peacemaker, sometimes it is still in the role of a victim. The real situation and the facts prove the opposite.

Russia annexed Abkhazia and Crimea. This allowed the aggressor to expand control over the Black Sea and carry out unprecedented militarization, modernizing the Black Sea Fleet in Sevastopol[3]. It also strengthened air defence and developed air systems. Russia can now easily wage hybrid war on any Black Sea country[4]. That's not all, Russia has deployed nuclear weapons in the region, 15 new warships in the Black Sea, some of them equipped with missile equipment[5].

It should be noted that Bulgaria, which is a member of the European Union and NATO, tries not to irritate Russia and avoids interfering in security issues. However, this does not exclude the possibility of cyber-attacks on this country by Russia. If any country in the Black Sea region tries to take a step that is unacceptable to Russia, it will have a war of appropriate strength at the expense of both military and cyber capabilities. In 2019, for example, Bulgaria bought eight new Lockheed Martin F16s for $ 1.256 billion from the United States, the largest military acquisition since the end of socialism. Bulgaria received cyberattacks in response. Hackers stole the personal financial data of thousands of Bulgarians and spread it by Russian e-mails. According to the leading Bulgarian newspaper 24 Chasa, the file was emailed by Russian hackers with more than 1.1 million identification numbers based on income, social protection, and health data[6].

Bulgaria supports cooperation and strengthening the military capabilities of coastal countries. There are a lot of problems in this country, including in the field of defence. Therefore, its positions are weak, especially on Black Sea security issues.

Both Georgia and Romania must be some of the main initiators of NATO activation in the Black Sea region. Romania has come up with an

---

[3] V. Socor, *The Black Sea Region: NATO's Exposed Sector on the Eastern Flank (Part Two)*, "Eurasia Daily Monitor", 2016, Vol. 13, Issue 114, pp. 117-118.

[4] S. Blank, *Memo to NATO: Wake Up Before Putin Turns the Black Sea into a Russian Lake*, <https://www.atlanticcouncil.org/blogs/ukrainealert/memo-to-nato-wake-up-before-putin-turns-the-black-sea-into-a-russian-lake/> (11.11.2020).

[5] *Russia to Respond to NATO Black Sea Force by Deploying New Weapons-Report*, <https://www.atlanticcouncil.org/blogs/natosource/russia-to-respond-to-nato-black-sea-force-by-deploying-new-weapons-report/> (12.11.2020).

[6] *Hackers Hit Bulgaria Sending Data From Russian Email*, <https://www.themos-cowtimes.com/2019/07/16/hackers-hit-bulgaria-sending-data-from-russian-email-a66431> (12.11.2020).

initiative to create a NATO-led Black Sea Fleet, which has received positive feedback. However, this issue has another side – the Russian factor. Romania's position and ideas are categorically unacceptable to Russia and have therefore become a hotbed of intense cyberattacks. The Romanian Defence Minister also stated at the Bucharest summit: "Romania is experiencing Russian aggression on the Black Sea coast daily. It avoids a wave of cyberattacks and political interference. Russia daily increases its military potential on the Crimean peninsula".

However, Romania has increased its defence spending from 1.81% to 2% of GDP and continues to support the strengthening of NATO positions in the Black Sea region, which means peace and stability. Nevertheless, we must admit that achieving peace and stability in the Black Sea basin is not an easy task, and even impossible shortly.

Turkey, which is interested in security, is also an important player in the Black Sea region. Turkey, like Bulgaria and Romania, is a NATO member and should show full support in the region, but that does not seem to be the case at all. There is the Montreux Convention, signed in 1936, which provides for the control of the Bosphorus Strait by Turkey. Although this document is in jeopardy in the face of Russian aggression, NATO's role in the region is strictly limited under this convention[7].

Turkey is trying to maintain balance and pursue its interests in the Black Sea region. In many cases, there are common interests with Russia, and cooperation with NATO is also mandatory. When Turkey does not behave the way Russia wants, the aggressor reveals his face here as well. With asymmetric and soft power technologies the Moscow is trying to harm Turkey. In this case, from the main topic of our article, we will focus on cyberattacks. For example, after Turkey shot down a Russian military plane over the Syrian border, Russian hackers launched DDoS attacks on Turkish Internet servers, shutting down government agencies, banks, and other commercial websites[8].

Let's go back to Ukraine and Georgia, where large-scale cyberattacks took place even after the conquest of territories – in 2017, the internal system of the Cabinet of Ministers of Ukraine was attacked by hackers. This was also stated by the Vice Prime Minister of Ukraine Pavel

[7] J. Bugajski, P. Doran, *Black Sea Defended: NATO Responses to Russia's Black Sea Offensive*, "Centre for European Policy Analysis", Strategic Report No. 2, July 2016.

[8] J. Global, *Turkish Internet Servers under Sustained Cyber Attack*, <https://jakartaglobe.id/news/turkish-internet-servers-sustained-cyber-attack/> (14.11.2020).

Rosenko: “It seems that the Secretariat of the Cabinet of Ministers of Ukraine has been attacked by hackers. The network is currently down.”[9]

At that time, not only the Cabinet of Ministers of Ukraine was the target of hacker attacks, but also the critical infrastructure. Ukraine is trying to escape from the shackles of Russia, but it fails. As for Georgia, it is also experiencing harassment, military provocations, as well as cybertechnologies, and information-propaganda manipulations. Russia's attitude towards Georgia and Ukraine is almost the same, but it differs from Bulgaria, Romania, and Turkey. As we have already mentioned, Russia avoids the direct confrontation with NATO member states.

There is a cybersecurity bureau in Georgia as well as a data exchange agency. These agencies work in the field of cybersecurity and try to respond quickly to cyber incidents. Nevertheless, large-scale cyberattacks are often carried out in Georgia. The country does not have the resources to protect itself from such cyberattacks. For example, after the 2008 Russia-Georgia war, cyberattacks took place in 2019, when the websites of Georgian government agencies went down and the country's leading TV stations were working with delay for several days, intending to steal confidential information and destroy TV archives[10].

Although three countries in the Black Sea region are members of NATO, it is still not possible to properly respond to Russian aggression and we can say that Russia has significant control over the Black Sea region – it uses various technologies and manipulations to influence the Black Sea countries and weaken their political aspirations.

NATO Cyber Security Capabilities and the Black Sea Region

When we say that Russian hegemony is raging in the Black Sea region, we cannot forget the other side – NATO, the European Union, the United States. Their support and steps towards peace are important events in the Black Sea region. Were it not for cooperation and various military, technological or financial supports, the situation in the Black Sea region would have been much worse. NATO and the EU are trying to deepen

[9] *Ukraine cyber-attack: Chaos as national bank, state power provider and airport hit by hackers, Russian energy firms and Danish shipping company also hit by hackers*, <https://www.independent.co.uk/news/world/europe/ukraine-cyber-attack-hackers-national-bank-state-power-company-airport-rozenko-pavlo-cabinet-computers-wannacry-ransomware-a7810471.html> (6.11.2020).

[10] *The cyber-attack in Georgia in October 2019 was carried out by the General Staff of the Russian Armed Forces*, <https://1tv.ge> (13.11.2020).

cooperation in the South Caucasus and specifically in the Black Sea region. There is also active cooperation in the field of cyber defence – conferences and practical training are held. Michael Gaul, senior advisor in NATO's Strategy and Projects Emerging Security Challenges Division, explains: "Cyber threats in this region often come from common sources and have many of the same characteristics, including the method of attack. Therefore, practical cooperation in the field of cyber defence between the Black Sea and South Caucasus partners can only guarantee their national and collective security."[11]

Security and cyberdefence, both globally and in the Black Sea region, are directly linked to NATO. The need to strengthen defence against cyberattacks was first discussed by NATO member states at a summit in Prague in 2002. Since then, cybersecurity has become an important component of NATO's agenda. In 2008, the first cyberdefence policy document was adopted. The process of integrating cybersecurity into the NATO defence system has been active since 2012. At the Wales Summit in 2014, the Allies made cyberdefence a key part of their collective defence, saying that a cyberattack could lead to the application of Article 5 of the NATO Treaty on Collective Defence. At the 2016 Warsaw Summit, Alliance member states recognized information and communication network security as one of their key defence areas and agreed that NATO must defend itself as effectively in cyberspace as it does on land, sea, and air. NATO's main partner in the field of cybersecurity is the European Union, with which the Alliance signed a technical agreement on mutual assistance and cooperation in February 2016[12]. At the 2018 Brussels Summit, the Allies agreed to set up a new cyberspace operations centre. Given the common challenges, NATO and the EU are strengthening cooperation in the field of cyber defence, especially in the exchange of information. Joint training and researches are conducted[13].

Of particular note is the merit of the United States, which spares no effort to develop new regulations on cybersecurity and also spares no

[11] *Enhanced cyber defence cooperation in the South Caucasus and Black Sea region*, <https://www.nato.int/cps/en/natohq/news_121969.htm> (15.11.2020).

[12] *NATO's Cyber Defence Evolution – NATO's New Digital Wall*, <https://russiancouncil.ru/en/analytics-and-comments/analytics/evolyutsiya-kiber-oborony-nato/> (16.11.2020).

[13] *Brussels Summit Declaration – Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Brussels 11-12 July 2018*, <https://www.nato.int/cps/en/natolive/official_texts_156624.htm?selectedLocale=en>

funds. Expenditures on cybersecurity in the U.S. budget are increasing every year. It is already known that by 2021 this sector will be funded with 18.8 billion dollars[14].

Conclusion

At the 2018 Brussels Summit and the Ministerial of Defence, special attention was paid to ensuring the security of the Black Sea and deepening practical cooperation with Georgia in this process. The Substantial NATO-Georgia Package (SNGP) has been developed under the auspices of the Ministry of Internal Affairs of Georgia. Under the package, the Border Police Coast Guard Department will train two boarding teams and implies involvements in the NATO Operational Capabilities Concept (OCC) process. This is already a step forward in terms of strengthening maritime security in the region.

If the alliance accelerates its expansion in the Black Sea region, of course, Russia will become more aggressive, but the process should not be stopped. At this stage, Ukraine and Georgia have the same problems, which one of the main obstacles in terms of NATO membership – is the occupied territories. Unfortunately, these problems cannot be solved. In this case, it is necessary to develop a new scheme that will set Russia at least the same red line as it has imposed on member states. Cybersecurity does not and cannot be localized in any one space. It is a war without borders. Russia or other harmful actors can be eliminated only through joint efforts, cooperation, and at the same time strengthening own cyber technologies. This includes training, as well as the development and refinement of new security systems.

Bibliography:

- ✓ Blank S., *Memo to NATO: Wake Up Before Putin Turns the Black Sea into a Russian Lake*, <https://www.atlanticcouncil.org/blogs/ukrainealert/memo-to-nato-wake-up-before-putin-turns-the-black-sea-into-a-russian-lake/>
- ✓ *Brussels Summit Declaration – Issued by the Heads of State and*

[14] *Department of Homeland Security Statement on the President's Fiscal Year 2021 Budget*, <https://www.dhs.gov/news/2020/02/11/department-homeland-security-statement-president-s-fiscal-year-2021-budget> (17.11.2020).

Government participating in the meeting of the North Atlantic Council in Brussels 11-12 July 2018, <https://www.nato.int/cps/en/natolive/official_texts_156624.htm?selectedLocale=en>

- ✓ Bugajski J., Doran P., *Black Sea Defended: NATO Responses to Russia's Black Sea Offensive*, "Centre for European Policy Analysis", Strategic Report No. 2, July 2016
- ✓ *Department of Homeland Security Statement on the President's Fiscal Year 2021 Budget*, <https://www.dhs.gov/news/2020/02/11/department-homeland-security-statement-president-s-fiscal-year-2021-budget>
- ✓ *Enhanced cyber defence cooperation in the South Caucasus and Black Sea region*, <https://www.nato.int/cps/en/natohq/news_121969.htm>
- ✓ *Hackers Hit Bulgaria Sending Data From Russian Email*, <https://www.themoscowtimes.com/2019/07/16/hackers-hit-bulgaria-sending-data-from-russian-email-a66431>
- ✓ *NATO's Cyber Defence Evolution – NATO's New Digital Wall*, <https://russiancouncil.ru/en/analytics-and-comments/analytics/evolyutsiya-kiberoborony-nato/>
- ✓ *Russia to Respond to NATO Black Sea Force by Deploying New Weapons-Report*, <https://www.atlanticcouncil.org/blogs/natosource/russia-to-respond-to-nato-black-sea-force-by-deploying-new-weapons-report/>
- ✓ Russian National Security Strategy, *Edict of the Russian Federation President – On the Russia Federation's National Security Strategy*, Moscow 2015
- ✓ Socor V., *The Black Sea Region: NATO's Exposed Sector on the Eastern Flank (Part Two)*, "Eurasia Daily Monitor", 2016, Vol. 13, Issue 114
- ✓ *The cyber-attack in Georgia in October 2019 was carried out by the General Staff of the Russian Armed Forces*, <https://1tv.ge>
- ✓ *Ukraine cyber-attack: Chaos as national bank, state power provider and airport hit by hackers, Russian energy firms and Danish shipping company also hit by hackers*, <https://www.independent.co.uk/news/world/europe/ukraine-cyber-attack-hackers-national-bank-state-power-company-airport-rozenko-pavlo-cabinet-computers-wannacry-ransomware-a7810471.html>