



EASTERN REVIEW 2020, T. 9


Vakhtang Maisaia

 <https://orcid.org/0000-0003-3674-3570>
Caucasus International University, Tbilisi, Georgia
Faculty of Social Sciences
e-mail: vakhtang.maisaia@ciu.edu.ge

Alika Guchua

 <https://orcid.org/0000-0003-0347-9574>
Caucasus International University Tbilisi, Georgia
Faculty of Social Sciences
e-mail: alikaguchua7@gmail.com

Thornike Zedelashvili

 <https://orcid.org/0000-0003-2630-1779>
Caucasus International University, Tbilisi, Georgia
Faculty of Social Sciences
e-mail: ThomasZedelashvili@gmail.co

The cybersecurity of Georgia and threats from Russia

Abstract. The world is living in a state of constant psychological warfare, technological advances and development; in the 21st century Internet governance has become a puzzle for scientists and practitioners. Virtual warfare is an alternative to real warfare, one of the biggest threats to global security. In discussing the issue, we must consider the capabilities of the world's leading countries, and first of all, identify the threat posed by Russia, which is the core of unpredictable aggression. This state is trying to influence almost the whole world with large-scale cyber-hacking attacks and continuous disinformation and fake news. Today it is difficult to find out where the theoretical war begins and where the practical military aggression ends, so new research, recommendations, scientific papers, and defence strategies are needed. Defensive mechanisms are created for cyber-attacks and this is always followed by more powerful attacks; that is why NATO enacted Article 5 of the Washington Treaty or the principle of "collective defence." The article discusses Russia's aggressive policy towards Georgia during and after the Russian-Georgian war in August 2008. The features of the Russian hybrid war and cyber attacks are discussed.

Keywords: Asymmetric threat, Technological advances, Cyber war, Information war, Hybrid war, Georgia, Russia, International security, Virtual space, Global security.

Introduction

Technologies are evolving in international politics and their use also poses a threat to malicious activity. The era in which we exist is within the daily regime of technological revolutions. With new technologies, powerful and more flexible defensive and offensive mechanisms are born. Cyber-attacks have become an integral part of our lives and an accompaniment to all military wars.

Cyberwarfare, as an event, began with the invention of the computer and the Internet. How was the computer created? This did not happen suddenly – it was based on the development of calculating technologies. The effective work of science in the twentieth century led to a technological revolution. For example, paper, magazine, newspaper, book, movie, and television have become as accessible as ever. This was followed (from 1950) by the serial production of computers and (in 1969) the first Internet connection. In 1989, the concept of the World Wide Web, known as the Web, was introduced in Europe. The idea of this concept meant not only the exchange of information through the Internet but also the posting of information by users. This is how websites are created, which is of great importance today. That's how we got to computer viruses, cyber-attacks and cyberwars. (National Academies Press, n.d.: 169–182).

What is the situation today and what problems has the technological revolution posed to us? Humanity has no way to slow this down – the fact is that the higher the level of computer technology, the greater the danger posed by cybercriminals. To better understand what we are dealing with let us consider the theory of cyber warfare and its place in modern politics. An important factor is the consideration and analysis of cyber threats and risks that Russia poses to the international community.

The main goal of the study is to discuss cybersecurity in Georgia, as well as analyze and present the threats posed by Russia. The research process uses comparative historical analysis and policy analysis to better identify and analyze Georgia's cybersecurity, as well as threats and risks from Russia.

The theory of cyber warfare and its place in modern world politics

When we talk about cyber warfare, we must first explain what event we are dealing with. It is one country's use of digital attacks on another (computer viruses or hacker cyber-attacks) to damage, liquidate and destroy computer infrastructure.

Experts have different opinions about the term “**cyberwar**”. Some say that the term “**cyberwar**” is incorrect because no cyber-attack recorded so far can be described as “war”. Whilst the second group believes that this is exactly the

appropriate name because a cyber-attack causes physical harm to people and objects in the real world.

Is cyber-attack considered a product of war? It depends on many factors – what they do, how they do it and what damage they do to the target object. Attacks must be of a significant scale and severity. Attacks by individual hackers or a group of hackers are not considered cyber warfare unless the state assists or directs them. Nevertheless, the virtual world is still vaguely represented in the direction of cyber-attacks. There are states that support hackers in carrying out malicious actions. This is a dangerous but common trend.

For example, cybercriminals who destroy banking computer systems while stealing money are not considered to be committing cyber warfare, even if they are from another country, but state-backed hackers doing the same to destabilize another country's economy are considered to be conducting cyber warfare.

There is also a difference between the target object and the scale: the “spoilage” of an individual company's website is not considered cyber warfare, but the malfunction of missile defence systems at an airbase is perceived as cyber warfare. In this case, it is important what weapon the attacker uses. For example, launching a rocket at a data centre would not be considered cyber, even if the data centre contained secret government records. Using hackers for espionage or data theft does not imply cyber warfare and it is defined by cyber espionage qualifications. There are many dark holes in cyber warfare.

Although there are differing views in this regard, today many countries – for example, the United States, Russia, Britain, India, Pakistan, China, Israel, the Islamic Republic of Iran and North Korea – already have enhanced cyber capabilities for both offensive and defensive operations.

Cyberwarfare is becoming an increasingly common and dangerous phenomenon in international conflicts. The fact that there are no clear rules may make virtual space uncontrollable in the nearest future.

During cyber wars, for the most part, computer systems are not the ultimate target, they are aimed at the infrastructure in the real world managed by such systems – airports, power grids, military units, and so on; such infrastructure is important for all countries. Pressing a button can close airports, subway stations and cut off electricity supplies.

There are many scenarios of cyber warfare: you may wake up one day and your bank accounts get lost because someone hacker wanted to cause this. In the case of mass attacks, it is possible to cause chaos in any country.

There are three main methods of cyber warfare: diversion, electronic espionage or stealing information from computers through viruses and attacking power grids. The third is probably the most alarming, implying a cyber-attack on critical infrastructure (Lewis University, 2016).

The methods of cyber-attacks are growing and improving every year. Back in 2006, the **Russian Business Network (RBN)** began using malicious programs to

steal personal data. Since 2007, the **RBN** has completely monopolized the online theft of personal data. By 2007, a virus called **Storm Worm** was operating on about one million computers and sending millions of infected emails every day. In 2008, cyber-attacks shifted from personal computers to government institution systems. On August 27 of the same year, **NASA** confirmed that a “storm worm” was found on laptops in the International Space Station. We cannot say for sure, but three months later the Pentagon computers were allegedly hacked by **Russian hackers**. Then there were the financial institutions, on December 25, 2008, there was an attack on the State Bank of India (Lewis University, 2016).

Russia has carried out and continues to carry out combined military and cyber-attacks against both **Georgia** and **Ukraine**, using various components of a hybrid war. The Kremlin did not change the Soviet methodology, it only changed the technologies. If we look at the issue in terms of crimes committed by Russia and still “not committed”, probably everyone recognizes that in this regard we are dealing with an unpredictable state. The leading countries of the world are obliged to turn the actions of this unpredictable country into a unified system and to resist.

In August 2008 (during the Russia-Georgia war), the largest cyber-attack was carried out by Russia on the websites of Georgian state, television and news agencies. A similar example can be given in relation to the Russia-Ukraine war in 2014, where the military war was accompanied by various components of the hybrid war – the so-called use of unidentified “Titushki” and cyber-attacks on government agencies. A few years later, in 2017, the internal system of the Cabinet of Ministers of Ukraine was attacked by hackers. Ukraine’s Deputy Prime Minister, Pavel Rosenko, wrote on Twitter: “It seems that the Secretariat of the Cabinet of Ministers of Ukraine has been attacked by hackers, the network is currently down” (Independent, 2017).

At that time, not only the Cabinet of Ministers of Ukraine was the subject of attack by hackers, but also the work of energy companies and the National Bank. At the same time, the media holding “Lux”, the Kiev metro, the Ukrainian Post and others were victims of cyber-attacks. As it was later reported, among the targets was the Boryspil airport system, through which flights can be delayed.

The concept of cyber warfare and the 21st century international security system

When we talk about the concept of cyber warfare and security, we must consider it in the context of the North Atlantic Alliance program – security and cyber defence are directly related to NATO. The need to strengthen cyber defence was first discussed by NATO members at a summit in Prague in 2002. This topic has since become an important component of the NATO agenda. In 2008, the

first cyber defence 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 cyber defence a key part of their collective defence, saying that a cyber-attack could lead to the application of Article 5 of the Collective Defense Treaty set out in the NATO Treaty. At the 2016 Warsaw Summit, Alliance member states recognized information and communication network security as a key area of defence 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 (RIAC, 2016).

The main issues discussed at the Warsaw Summit were how to allocate resources on cybersecurity to achieve the best effect – recognizing that large resources were needed to address this problem. Also, there were questions about how much money should be spent, – what would be the minimum level of investment? For example, since 2014, the budget of “**Pacte Défense Cyber**” in France has included 1 billion euros for cyber defence. In 2016, the UK announced it had allocated 1.9 billion pounds sterling to strengthen its cybersecurity program (Reuters, 2014).

At the 2018 Brussels Summit, the Allies agreed to set up a new cyberspace operations centre. Taking into account common challenges, NATO and the EU are strengthening cooperation in the field of cyber defence, especially in the exchange of information. Joint trainings and studies are conducted (NATO, 2018).

Of particular note is the merit of the United States, which spares no effort to develop new regulations on cybersecurity and also spares no funds. Expenditures on cybersecurity in the US budget increase every year, in 2015 the Barack Obama administration officially allocated \$14 billion, and then there was information that much more would be spent (CNet, 2015). Worldwide defence spending is rising day by day, but U.S. finances are impressive. It is already known that by 2021 this sector will be funded with \$18.8 billion (Homeland Security, 2020). Let us consider an important issue called the national security strategy that every country has and where it clearly shows the attitude of this or that country towards security. The national security strategy is the most important document for creating a safe environment for the state. Cyberwarfare plays an important role in the security strategies of the world's leading powers – for example, the United States, the United Kingdom, Russia, China, Iran, France, Spain, etc. This issue also occupies an important place in the National Security Strategy of Georgia.

What is interesting, is the view of the Russian government in terms of global threats. In the 2015 version of the Russian National Security Doctrine, the 16th and 17th paragraphs consider the United States and NATO as the main opponents, while the 7th paragraph directly states the role of the Russian Federation in the maintenance of world order (Russian National Security Strategy, 2015: 1–4).

The Russian Federation says it does not even pose a threat to other countries, but is itself a victim and has systems in place to deal with threats from the US and NATO. The real facts, however, prove the opposite. For example, it was Russia that used the elements of “hybrid warfare” to deal a serious blow to the United States, adding signs of political instability to the monolithic political system of that country during the presidential election. Even if the story of hacker interference in the presidential election is a complete lie, at least Russia is benefiting, this fact shows that it is omnipotent, which is what causes the nihilism of the people of the United States. But why only the population of this country? When the whole of Europe, Asia or Africa sees that even a superpower is vulnerable at certain moments, everyone feels frustrated and helpless. One example is the terrorist attacks of September 11, 2001, in the United States. This is where not only “American nihilism” but “world nihilism” first appeared. It was during this period that the United States had the so-called Reset Policy – Secretary of State Hillary Clinton arrived in Moscow and presented a symbolic reset button to Russian Foreign Minister Sergei Lavrov. Whilst the security doctrine directly states that constructive cooperation with Russia is necessary, NATO-Russia security is essential. As we have seen later, such an approach did not work.

What exactly is written in the US National Security Strategy, published in December 2017? In the introduction to the strategy, it is stated that the well-being and security of the United States depend on how it responds to the opportunities and challenges in cyberspace. It also notes that critical infrastructure, national defence, and the daily lives of Americans rely on computer and information technology (United States of America, 2017: 1–2). That is, on the very first page of the US National Security Document, focus is placed on the important factors of cyber technology, which means that threats from cyberspace affect all areas and damage both tangibly and intangibly.

The world’s leading research and consulting firm **Gartner** publishes data on cybersecurity expenditures, which are compared and discussed by the 2017–2019 global cybersecurity expenditure segment.

We see in the table (Table 1) that in terms of cybersecurity, worldwide, very large sums of money are spent and this is growing every year. For example, spending in 2017 was \$101,544 billion; by 2018 it had increased to \$114,152 billion, and in 2019 it reached \$124,116 billion. According to **Gartner**, in 2022 global cybersecurity spending will reach \$133,7 billion. What is noteworthy, however, is the fact that the damage done to the world far exceeds the amount spent on security (Gartner, 2018).

The **Cybersecurity Ventures** report also estimates that cyber-attacks will cost \$6 trillion by 2021, up from \$3 trillion in 2015 (Morgan, 2017: 3).

Table 1. Data of the world-leading scientific-consulting company “Gartner” for 2017–2018–2019 in terms of cybersecurity costs

Market Segment	2017	2018	2019
Application Security	2,434	2,742	3,003
Cloud Security	185	304	459
Data Security	2,563	3,063	3,524
Identity Access Management	8,823	9,768	10,578
Infrastructure Protection	12,583	14,106	15,337
Integrated Risk Management	3,949	4,347	4,712
Network Security Equipment	10,911	12,427	13,321
Other Information Security Software	1,832	2,079	2,285
Security Services	52,315	58,920	64,237
Consumer Security Software	5,948	6,395	6,661
Total	101,544	114,152	124,116

Sources: Gartner, 2018.

Russian cyber attacks against Georgia

In August 2008, Russia carried out acts of aggression against Georgia on two fronts – a real military attack and a surreal, that is, virtual attack on the Internet. Before the real war started, Russian hackers actively attacked the websites of state agencies. According to official information, the cyber-attack took place on about 60 websites. Most of them featured propaganda exhortations, photos of former President Mikheil Saakashvili being equated with Adolf Hitler.

Was this cyber-attack unexpected for Georgia and the international community? As further assessments showed, the attack was not unexpected, but no one expected such a strong attack. It was later evaluated as a lesson. Former government officials say that then, with the help of international partners, state websites were transferred to American servers and the problem was solved, but the issue remained open – Russia reached its goal, seizing both the real military training ground and the Internet. The investigation of the Ministry of Defence of Georgia revealed that the attack was prepared two years before the war. Former Deputy Defence Minister Batu Kutelia says there are a number of facts to prove this:

Cyber-attacks were carried out from web platforms that previously served criminals. Specifically, these were dark webs that are a platform for Russian organised crime. The deface used in the attack included specific keywords: NATO, Georgia and the United States, and military cooperation. In addition, several defaces, made two years before the war, were simply activated in 2008 (Agency “on”, 2019).

According to Andria Gotsiridze, a cyber-security expert, the DoFS cyber-attacks against Estonia and Lithuania in 2007–2008 were a punitive operation and a kind of political message aimed at provoking civil and mass unrest. However, it was not related to the performance of this or that military task, nor did it serve as information support for hostilities. As for the Russia-Georgia war, the use of the cyber element here was a process directly accompanied by conventional actions aimed at facilitating the fulfilment of Russian Armed Forces military objectives, creating an information vacuum, and thus gaining an information advantage and establishing a Russian narrative of the conflict (Gotsiridze, 2019).

Cyber-attacks from Russia do not happen every day. However, the fact is that Russian propaganda is constantly growing and is also recorded at the official level in the reports of the State Security Service. According to experts, the Kremlin has not only softened the tone but also applied the principle of decentralisation – creating small marginal groups that spread radical views. This is like an attack when a lot of information comes together, the server overloads and stops. Pro-Western NGOs also point out in their reports that another important support of Kremlin propaganda in Georgia is the recent proliferation of pro-Russian NGOs, most notably the **Eurasian Institute** and the **Eurasian Choice** (IDFI, 2016).

According to them, these organisations are distinguished by their anti-Western rhetoric and rely on Russian sources when publishing analytical papers or articles. According to the public registry, the list of founders and heads of pro-Russian NGOs often includes the same people. The link between the organisations is also indicated on their websites. In addition, a network of pro-Russian NGOs has links to anti-Western rhetorical media. Pro-Western NGOs may not be lying in part, but the organisations they name claim that the opposite is true – the Western course is being thwarted by organisations that are presented with fake pro-Western packaging. If the so-called “Eurasian” organisations do not hide their orientation and often say that they are doing business, not for Russia, but for Georgians, in pro-Western organisations, it is often really difficult to find out – there are cases when personal interests are clearly observed in the research of this or that issue.

Some non-governmental organisations also write that pro-Russian political parties have multiplied in Georgia. Statements are often made as if a number of political parties and politicians, directly or indirectly, are spreading propaganda useful to the Kremlin. Political parties are divided into two parts: firstly – they have an openly pro-Russian agenda, meet with Russian politicians and visit Moscow; Secondly, parties that, at the declaration level, distance themselves from the Russian political elite and instead declare themselves pro-Georgian, pro-neutral parties. Despite the differences, the basic messages of both political parties are the same – their calls for membership of European and Euro-Atlantic structures arouse scepticism. Georgia’s aspirations towards Western institutions are presented as fruitless, like a dream. Instead, the idea of pro-Russian sentiment and Georgia’s neutrality is being popularized.

Some of the non-governmental organizations suspect that clergymen are also involved in the anti-Western campaign. They spread the myth that Georgian traditions are incompatible with Western culture. Some clerics in their sermons develop the idea of civilizational unity with Russia and ideological or moral opposition to the West. Indirect or direct dissemination of Kremlin propaganda messages is a serious problem, and the clergy have high trust and influence in Georgian society. According to pro-Western NGOs, this cannot be accidental. It turns out, the public likes and recognizes their orientation. If the public is fascinated by such sermons, then the problem is partly with the population.

It is obvious that Russia is the source of many problems for Georgia, but in a small part of the society there is another kind of illusion: firstly, many preach that Russia will be disintegrated day by day, emptied and we will be saved; secondly – a democratic government will come to Russia and we will annex the territories without any problems; thirdly, Russia will soon run out of oil, go bankrupt and we will also be saved. Maybe someday everything will happen, but with such considerations, we cannot go far. What will be in store for humanity following the collapse of Russia and also what will follow the advent of democratic government in Russia, no one knows yet.

On this background, there is a virtual threat – cyberwar and the information front, which is open in several directions. One is open propaganda, the other is disguised propaganda, that is, pursuing Russia's interests through pro-Western shields. Russia attacks the United States, the Baltic States, Ukraine, Georgia, Europe, and the rest of the world with cyber-methods, pre-processed hybrid methods and disinformation. For example, Russians in Slovakia and the Czech Republic are critical of US energy policy and try to portray the US as acting solely in its own interests, provoking conflicts in various parts of the world. In Romania, Russian-funded media outlets are trying to misrepresent EU membership and undermine democratic institutions. In Sweden, the government is portrayed as a follower of sexual depravity. Propaganda supporting the premise of corruption, poverty, disorder and the Western-backed "puppet" regime is spreading in Ukraine. In Lithuania, Latvia and Estonia, the propaganda machine works on how discriminated against Russians are in these countries because of their ethnic or linguistic characteristics (Institute for Development of Freedom of Information, 2016: 5–33).

Despite Russian aggression, it must be said of all post-Soviet countries that mass persecution of Russians and the Russian-speaking population did not occur after the collapse of the Soviet Union, no bloodshed and cruelty took place. Perhaps the decisive factor, in this case, was the fact that at least 70 years of kinship and other cultural or social relations were formed. Instead of Russia taking care of these relations, it began to create a space similar to the Soviet Union, where it is constantly carrying out military aggression and waging a hybrid war. It is known that the main driving force of Russian propaganda in the Baltics is the "First

Baltic Channel”, as well as the online site **Regnum.ru**, which has been operating for more than 10 years. Recently, the Russians launched the site Baltnews, which anonymously publishes information and news in the Estonian, Lithuanian and Latvian languages (Agency “Independence”, 2015).

According to the German edition of *Bild*, citing its own sources, if the United States had openly intervened in the 2008 Georgian-Russian war, the Russians had decided to attack the Baltic States and if the Americans were to help the Baltic States, then they would consider using nuclear weapons. The *Bild* reviewer also writes that as part of a large-scale military exercise – “Western 2017”, Russia rehearsed not in the fight against terrorism, but in the war against NATO, and they have this information based on Western intelligence. The publication claims that the training scenario was based on the occupation of the Baltic States and Belarus in a few days. The exercise also involved a “shock campaign” against NATO member states, including Germany, the Netherlands, Poland, Norway, neutral Sweden and Finland. According to the source, Russia was training to neutralize and control the airports and ports of the Baltic States. There is an excerpt from the publication:

If the war were to actually take place, their goal would be to build critical infrastructure, including airports, ports, stations and other infrastructure, to cause shock in these countries and for locals to demand a truce from the government (German newspaper *Bild*, 2017).

According to the publication, as part of the exercise, Russia tested the bombing and capture of the Norwegian city of Spitsbergen. As we have seen, this plan did not materialize, the United States did not succumb to Russian provocation in the events of 2008; but since there is a similar model plan, Russia is still doing its job with hybrid warfare and cyber-attacks. Do not rule out that the same crisis situation will arise again.

In June 2018, the Pentagon acknowledged that in the event of a Russian invasion, it would not be able to defend the Baltic States and Poland. According to the “Washington Post”, this conclusion was reached at the Pentagon as a result of simulating military resistance between EU countries and Russia. According to the publication: “Russia will be able to occupy the Baltic states before the US Army headquarters completes 17 forms to move NATO advanced forces from Germany to Poland.” The newspaper writes that another major problem for the US military is the narrow streets and unreliable transport infrastructure, even the bridges are so weak that they cannot withstand the weight of American equipment. European bureaucracy also creates problems at the borders (*The Washington Post*, 2018).

Russia has opened several fronts in the post-Soviet space, involving high-ranking government officials. For example, in September 2019, Foreign Minister **Sergei Lavrov** noted that the Baltic States are still living on EU subsidies and their assistance will soon cease (Iagorashvili, 2019). Of course, this is deliberate

disinformation, through which the Russians are trying to install nihilism and despair in the people of the Baltic States – Hey, the EU is helping you today, you are on the provision of the West, but tomorrow it will stop helping you – Russia is exerting constant ideological, pressure for example the Kremlin has consistently argued that the sovietisation of the Baltic States was in accordance with international law and that the term “**occupation**” could not be used there. The Kremlin is hiding the fact that when the foreign ministers of these countries did not want to sign the so-called agreement, they feared that Russia would violate their neutrality. After the refusal, **Molotov** addressed the representative of Estonia as follows:

We cannot wait long. I advise you to agree to the Soviet Union’s wish to avoid worse. Do not force the Soviet Union to use force (Iagorashvili, 2020).

This is the same “invitation” of the Russian troops as the Bolsheviks under the command of **Sergo Orjonikidze** were “invited” to Georgia. Falsifying history – this is another direction of Russia, or part of a larger strategy, which “fits” perfectly within the framework of the hybrid war.

Russia is at the forefront in terms of cyber capabilities. What is the Russian cyber power and what is its role? Russia has been really innovative in various conflicts. Due to the specific geopolitical environment, Russia has successfully adapted cyber-attacks to expand its interests. One of them is the 2007 cyber-attacks against Estonia. It was a simple **DDoS** attack that did not cause significant damage but had a positive impact on **strengthening Estonia-NATO relations in terms of security**. The same thing happened in 2008 during the **Russia-Georgia war**, which has been discussed in-depth in our article. As well as in **Ukraine**, where cyber-attacks have been more “sophisticated” and damaging. There are many examples that point to **Russia’s** enhanced cyber capabilities. Cyber-attacks carried out by **Russia** are mostly used in conditions of asymmetric conflict. However, the interference of hackers in the **US** presidential election in 2016 was different in the sense that it was intended to test cyber capabilities in order to influence the election. Naturally, **Russia’s** capabilities also have a limit. When carrying out a cyber-attack with a certain strategy, potential opponents have the opportunity to prepare in a defensive direction. **Russia’s** cyber-attacks on **Georgia** and **Ukraine** may be considered experiments, but it **allows leading countries** to fully explore the so-called **Russian** methods in technological terms. And then it becomes easier to improve defence mechanisms. For example, the interference of **Russian** hackers in the elections in **France, Italy, the Netherlands** and **Germany** was not as effective as it may have been in previous cases. The threats posed by Russia are multifaceted, both in terms of cyber warfare and the use of information and propaganda disinformation. The phenomenon of **the information-propaganda war** is not new, it just progressed and probably will continue to progress with the development of technology.

Propaganda – means the planned use of any form of communication to influence people’s minds, behaviours and emotions. This means is considered by many to be the most effective and common means of persuading people to engage in political activity. Intelligence services have thus been employing propaganda for a long time. The full force of the **propaganda war** was revealed during the **Second World War** and is still relevant today. In this regard, we can say that Russia has a long history of information, propaganda and disinformation, but in the era of technological revolutions, this activity has become more effective. Russian **propaganda** is not truth-oriented, but that does not mean that everything is a lie. Here we have a mixed-method when mixed misinformation is spread encompassed in truth. There are cases when we are dealing with complete disinformation and “**fake news**”. For example, a fake report on September 11, 2014, informing us that a **chemical** plant in **Louisiana** had exploded (Manufacturing, 2015). At the time this information seemed credible, it appeared on almost every social network. Generally, fake news spreads quickly and is easily believed, especially when the information is spread by not one, but several media outlets. In this case, it is important to warn the public about impending misinformation.

The mainstay of Kremlin propaganda in Georgia is the media and social networks. At least one television station, several Internet TV stations, print media and a web site feature anti-Western message boxes that rely heavily on Russian sources of information. The active use of social networks by Russian propagandists is also noticeable in the viral dissemination of disinformation or anti-Western narrative materials.

In May 2013, the President of Georgia signed the **Cyber Security Strategy of Georgia** for 2013–2015, which is the main document defining state policy in the field of cybersecurity (Administration of the President of Georgia, 2013: 1–9).

Georgia’s National Cyber Security Strategy states separately that it is necessary to raise public awareness and establish an educational base. It is also emphasized that our public awareness is quite low. Raising awareness is also a big challenge for the public sector, where a significant part of the employed officials do not have the knowledge of the basic norms of cybersecurity and need to be trained. The Georgian security strategy or plan openly recognizes that today it is impossible to ensure cybersecurity on its own, because cyber incidents have already become transnational and in this case, it is necessary to join the international system. Here again, we go to the plans and experience developed by NATO and the US, and then to the cooperation (Resolution of the Government of Georgia № 14, 2017: 6–7).

On February 6, 2014, on the basis of order No. 8 of the Minister of Defence of Georgia, the LEPL “**Cyber Security Bureau**” was established and its statute was approved. Cybercrime investigation is one of the most important issues in terms of the proper functioning of the state. This requires a proper technical and legal framework, qualified staff, cooperation with partner countries and so on.

Given Russia's aggressive intentions and policies in modern times, it is imperative that Georgia, Ukraine and their Western partners strengthen their defences and share their experiences and technologies.

Conclusion

The trend of cyber wars and covert cyber-attacks has recently taken on a larger scale and is undergoing a transformation. At a closed meeting of the UN Security Council in 2020, the United States and Britain openly blamed Russia. The facts were also presented. Estonia, Ukraine and Georgia were discussed at the meeting. Since Estonia is a member of NATO, it automatically shares the concept that has already been developed and provides for inclusion in the collective defence system (Georgian Public Broadcaster, 2020). As for Georgia and Ukraine, the NATO plan works effectively in this case as well, but in the end, at least individual methods of defence need to be strengthened. Especially when the Georgian state is a constant target for Russia. The fact is that Russia in the post-Soviet space feels like a fish in water, which can be controlled only through international efforts. Georgia has high hopes for its European partners and the United States in protecting Georgia from cyberattacks and hybrid wars. While it is difficult for rather powerful states to cope with the threats and risks posed by Russia, the support of Western partners is important to protect and strengthen Georgia's security. As a result of the study, we can say that the cybersecurity environment of Georgia reacts to a certain extent to the threats posed by cyberspace.

References

- Administration of the President of Georgia. 2013. Decree of the President of Georgia. *Cyber Security of Georgia* 321, pp. 1–9, <https://matsne.gov.ge/ka/document/download/1923932/0/ge/pdf> (accessed 8.10.2020).
- Agency "Independence". 2015. *Russian Information War – Strategies and Goals*, p. 1. http://damoukidebloba.ge/c/news/sainformacio_omi (accessed 2.10.2020).
- Agency "on". 2019. *How we repelled cyber-attacks and propaganda in 2008*, p. 1, <https://on.ge/> (accessed 6.10.2020).
- CNet. 2015. *Obama asks for \$14 billion to step up cybersecurity*. The president urges Congress to pass legislation that would strengthen the country's hacking detection system and counterintelligence capabilities, p. 1, <https://www.cnet.com/news/obama-adds-14b-to-budget-for-stepped-up-cybersecurity/> (accessed 10.10.2020).
- Gartner. 2018. *Gartner Forecasts Worldwide Information Security Spending to Exceed \$124 Billion in 2019*. p. 1, <https://www.gartner.com/en/newsroom/press-releases/2018->

- 08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019 (accessed 15.10.2020).
- Georgian Public Broadcaster. 2020. *US, Britain and Estonia discuss Russia's cyber-attacks against Georgia at closed-door UN Security Council meeting*. p. 1, <https://1tv.ge/news/gaero-s-ushishroebis-sabchos-dakhurul-skhdomaze-ashsh-ma-britanetma-da-estonetma-saqartvelos-winaaghmddeg-rusetis-kibertavdashkmebze-isaubres> (accessed 17.10.2020).
- German newspaper *Bild*. 2017. German media: The Russians intended to use nuclear weapons in 2008. Retrieved from German media: The Russians intended to use nuclear weapons in 2008, p. 1, http://www.resonancedaily.com/index.php?id_rub=2&id_artc=42590 (accessed 11.10.2020).
- Gotsiridze, A. 2019. *Cyber-dimension of the Russia-Georgia war of 2008. Cyber-dimension of the Russia-Georgia war of 2008*, p. 1, <https://www.gfsis.org/ge/blog/view/970> (accessed 14.10.2020).
- Homeland Security. 2020. *Department of Homeland Security Statement on the President's Fiscal Year 2021 Budget*, p. 1, <https://www.dhs.gov/news/2020/02/11/department-homeland-security-statement-president-s-fiscal-year-2021-budget> (accessed 18.10.2020).
- Iagorashvili, I. 2019. *(Statement by Sergei Lavrov) Russia's Two Myths about the Baltic States*, p. 1, <https://www.mythdetector.ge/ka/myth/rusetis-2-miti-baltiispiretis-kveqnebis-shesakheb> Last checked (accessed 23.10.2020).
- Iagorashvili, I. 2020. *(Statement by Vyacheslav Molotov) Maria Zakharova denies the occupation of Estonia by the USSR*. Retrieved from (Statement by Vyacheslav Molotov), p. 1, <https://www.mythdetector.ge/ka/myth/maria-zakharova-ssrk-mierestonetis-okupatsias-uarqops> (accessed 23.10.2020).
- IDFI. 2016. *Kremlin Information War against Georgia: The Necessity of State Policy to Combat Propaganda*. Retrieved from Kremlin Information War against Georgia: The Necessity of State Policy to Combat Propaganda, p. 1, <https://idfi.ge/ge/informational-war-of-kremlin-against-georgia-the-necessity-of-having-state-policy-against-propaganda> (accessed 22.10.2020).
- Independent*. 2017. Ukraine cyber attack: Chaos as national bank, state power provider and airport hit by hackers, Available at Russian energy firms and Danish shipping company also hit by hackers, p. 1, <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> (accessed 20.10.2020).
- Institute for Development of Freedom of Information. 2016. *Kremlin Information War on Georgia: The Necessity of State Policy to Combat Propaganda*, Available at Policy Paperm, pp. 5–33, <https://idfi.ge/public/upload/Meri/Russian%2> (accessed 22.10.2020).
- Lewis University. 2016. *THE HISTORY OF CYBER WARFARE - INFOGRAPHIC*. A The New Face of War: Attacks in Cyberspace, p. 1, https://www.visualistan.com/2016/01/the-history-of-cyber-warfare-infographic_16.html (accessed 24.10.2020).
- Manufacturing. 2015. *Report: Russian 'Internet Trolls' Behind Louisiana Chemical Explosion Hoax*, pp.1–9, <https://www.manufacturing.net/operations/news/13099148/report-russian-internet-trolls-behind-louisiana-chemical-explosion-hoax> (accessed 24.10.2020).

- Morgan, S. 2017. *2017 Cybercrime Report*. report from Cybersecurity Ventures, p. 3, <https://cybersecurityventures.com/2015-wp/wp-content/uploads/2017/10/2017-Cybercrime-Report.pdf> (accessed 25.10.2020).
- National Academies Press. n.d. *7 Development of the Internet and the World Wide*, pp. 169–182, Available at *Funding a Revolution: Government Support for Computing Research* (1999), <https://www.nap.edu/read/6323/chapter/9> (accessed 26.10.2020).
- NATO. 2018. *Brussels Summit Declaration*. Retrieved from Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Brussels, p. 1, https://www.nato.int/cps/en/natohq/official_texts_156624.htm (accessed 26.10.2020).
- Resolution of the Government of Georgia № 14. 2017. *On the Approval of the National Cyber Security Strategy of Georgia for 2017–2018 and its Action Plan*, pp. 6–7, http://gov.ge/files/469_59439_212523_14.pdf (accessed 28.10.2020).
- Reuters. 2014. *France to invest 1 billion euros to update cyber defences*, p. 1, <https://www.reuters.com/article/france-cyberdefence-idUSL5N0LC21G20140207> (accessed 27.10.2020).
- RIAC. 2016. *NATO's Cyber Defense Evolution*. NATO's New Digital Wall, p. 1, <https://www.nato.int/docu/rdr-gde-prg/rdr-gde-prg-eng.pdf> (accessed 27.10.2020).
- Russian National Security Strategy. 2015. *EDICT OF THE RUSSIAN FEDERATION PRESIDENT*. Retrieved from *On the Russian Federation's National Security Strategy*, pp. 1–4, <http://www.ieee.es/Galerias/fichero/OtrasPublicaciones/Internacional/2016/Russian-National-Security-Strategy-31Dec2015.pdf> (accessed 28.10.2020).
- United States of America. 2017, december. *National Security Strategy*, pp. 1–2, <https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf> (accessed 29.10.2020)..
- The Washington Post*. 2018. The Pentagon has acknowledged that in the event of a Russian invasion, it will not be able to defend the Baltic states and Poland, p. 1, <https://imedinews.ge/ge/msoflio/67383/pentagonma-agiara> (accessed 29.10.2020).