https://doi.org/10.18778/1427-9657.11.18

EASTERN REVIEW 2022, T. 11(2)

*Alika Guchua*
https://orcid.org/0000-0003-0347-9574
Caucasus International University Tbilisi, Georgia
Faculty of Social Sciences
e-mail: alika_guchua@ciu.edu.ge

*Thornike Zedelashvili*
https://orcid.org/0000-0003-2630-1779
Caucasus International University, Tbilisi, Georgia
Faculty of Social Sciences
e-mail: ThomasZedelashvili@gmail.com

# Challenges arising from cyber security in the dimension of modern global security (on the example of the Russia-Ukraine war)

**Abstract.** The challenges and threats from cyber security are increasing every day in the world. All this has a significant impact on international relations. When we are dealing with such a revolutionary development of technology as in the 21st century, it is already necessary for all states to have high-standard cyber security systems. This is not an easy issue to solve, because cyber security requires quite a lot of finances, human resources, and also specially trained professionals. Threats emanating from cyberspace need a proper response, in this case we have no choice, the whole world is facing danger. Cybercrime and the damage caused by it are increasing year by year. Also, all this affects a person psychologically and leaves a feeling of insecurity. The biggest problem is that aggressive states, terrorist organizations, non-state groups, large corporations, etc. are mostly involved in this virtual war (as in the real one). As an example, we can cite such an aggressor state as Russia, which carries out major cyber attacks against Ukraine, Georgia and other states whose cyber security systems are less protected. The transition of political,

Received: 23.10.2022. Verified: 17.01.2023. Accepted: 14.03.2023.

military, social or criminal processes into cyberspace has made cyber security one of the main segments of state security. Countries with developed cyber-offensive potential, primarily Russia, successfully use cyberspace both during war and conflict, as well as in peacetime, to gain geopolitical advantage. This article discusses the challenges and threats associated with the development of modern cyber and information technologies, analyzes the threats associated with the new information security capabilities of modern states, including cybersecurity. The aim of the paper is to present the role of cyber security in the Russia-Ukraine war and the threats arising from it. The following methods are used in the paper: methods of historical-descriptive, policy research and comparative analysis. The paper uses the theories of balance of power and securitization.

**Keywords:** Cyber security, Cyber technologies, NATO, European Union, Georgia, Russia, Ukraine, Cyber attack, Cyber war.

# Wyzwania wynikające z cyberbezpieczeństwa w wymiarze współczesnego bezpieczeństwa globalnego (na przykładzie wojny rosyjsko-ukraińskiej)

**Streszczenie.** Wyzwania i zagrożenia związane z cyberbezpieczeństwem rosną każdego dnia na świecie. Wszystko to ma istotny wpływ na stosunki międzynarodowe. Kiedy mamy do czynienia z tak rewolucyjnym rozwojem technologii, jak w XXI w., konieczne jest już posiadanie przez wszystkie państwa systemów cyberbezpieczeństwa na wysokim poziomie. Nie jest to łatwa kwestia do rozwiązania, ponieważ cyberbezpieczeństwo wymaga sporych nakładów finansowych, zasobów ludzkich, a także specjalnie przeszkolonych specjalistów. Zagrożenia płynące z cyberprzestrzeni wymagają odpowiedniej reakcji, w tym przypadku nie mamy wyboru, cały świat stoi w obliczu niebezpieczeństwa. Cyberprzestępczość i powodowane przez nią szkody rosną z roku na rok. Ponadto wszystko to wpływa na psychikę ludzi i pozostawia poczucie niepewności. Największym problemem jest to, że w tej wirtualnej wojnie (podobnie jak w prawdziwej) biorą udział głównie agresywne państwa, organizacje terrorystyczne, grupy niepaństwowe, wielkie korporacje itp. Jako przykład możemy przytoczyć państwo agresora, jakim jest Rosja, która przeprowadza poważne ataki cybernetyczne na Ukrainę, Gruzję i inne państwa, których systemy cyberbezpieczeństwa są mniej chronione. Przejście procesów politycznych, wojskowych, społecznych czy przestępczych do cyberprzestrzeni sprawiło, że cyberbezpieczeństwo stało się jednym z głównych segmentów bezpieczeństwa państwa. Państwa o rozwiniętym potencjale cyberofensywnym, przede wszystkim Rosja, z powodzeniem wykorzystują cyberprzestrzeń zarówno w czasie wojny i konfliktu, jak i w czasie pokoju do uzyskania przewagi geopolitycznej. W artykule omówiono wyzwania i zagrożenia związane z rozwojem nowoczesnych technologii cybernetycznych i informacyjnych, dokonano analizy zagrożeń związanych z nowymi możliwościami bezpieczeństwa informacyjnego współczesnych państw, w tym cyberbezpieczeństwa. Celem artykułu jest przedstawienie roli cyberbezpieczeństwa w wojnie rosyjsko-ukraińskiej i wynikających z niej zagrożeń. W artykule zastosowano następujące metody: metody historyczno-opisowe, badania polityki oraz analizę porównawczą, a także wykorzystano teorie równowagi sił i sekurytyzacji.

**Słowa kluczowe:** cyberbezpieczeństwo, cybertechnologie, NATO, Unia Europejska, Gruzja, Rosja, Ukraina, cyberatak, cyberwojna.

## Introduction

In contemporary international relations, states and international organizations face many threats and challenges. These threats are: terrorism, separatism, extremism, cybercrime, information war, hybrid war, drug trafficking, transnational organized crime, pandemic spread, etc. From these given threats and challenges, we highlight the issue of cyber security, which is very relevant along with other issues mentioned above. The scale of cyberspace is infinitely large and transformative. It covers all areas of human activity in which electronic technology is involved. It must be said that threats from cyberspace have become a big puzzle for the world. We have already mentioned that the leading states work in a coordinated and separate manner. They try to develop, implement and develop different methods and approaches. But this is not a one-time or multiple act, because it is a continuous process – as technologies develop, threats increase, and there is no end in sight. Different hacker groups attack private or international organizations, steal money, damage strategic infrastructure. Also, aggressor states that hire or train hackers as cyber-terrorists carry out attacks on critical infrastructures of other states. All this can bring any country to a miserable state. In order to better present the issue and the extent of the danger that the states are dealing with, we can cite one very small example. Notably, in June 2021, the FBI began tracking ransomware incidents specific to 16 areas of critical infrastructure. Those hit hardest were healthcare and public health 148 reported incidents, financial services 89, IT 74, critical manufacturing 65, and government facilities 60 (Foley, 2022: 1).

Cyber warfare and international terrorism pose a serious challenge to global security because they know no do not know borders. Action in cyberspace requires the rejection of the common assumptions related to time and space because such attacks, by means of modern information and communications networks, can be performed from anywhere in a very short time. The processes of globalization did not have the impact only on the achievements of civilization, but also on the development of new threats to the civilization. It is a fact that terrorism and national threats changed under the influence of the globalization process and the Internet information revolution. Strategic advantage no longer lies in the fighting power or geographical location, but in the information and knowledge. International cooperation and intelligence sharing are essential for an effective prevention of cyber threats (Duić *et al.*, 2017). Threats from cyber-terrorists, hackers, cyber-criminals and others are compounded by the factor of aggressive states that pose the greatest threat in cyberspace. An example of which is Russia's and its emanating cyber threats to Ukraine, Georgia, the European Union, NATO, etc.

## Protecting critical infrastructure from aggressive actors

In the 21st century, there is a tendency to blur the distinction between the state of war and peace. Wars are no longer declared, and when they start, they do not go according to the pattern we are used to. In terms of the scale of casualties and destruction, catastrophic social, economic and political consequences, such conflicts of a new type are comparable to the consequences of a real war itself. The role of non-military methods in achieving political and strategic goals has increased, which in a number of cases have significantly surpassed the force of arms in their effectiveness. Weapons based on new physical principles and robotic systems, unmanned aerial vehicles, weapons with artificial intelligence systems are being actively introduced into military affairs. In the near future, the creation of fully robotic formations capable of conducting independent combat operations is not ruled out. As the militaries of technologically advanced nations seek to apply increasingly sophisticated Artificial Intelligence and automation to weapons technologies, a host of ethical, legal, social, and political questions arise. Central among these is whether it is ethical to delegate the decision to use lethal force to an autonomous system that is not under meaningful human control (Asaro, 2020: 1).

The use of the cyber element in conflicts and interstate Interactions has undergone significant changes in the last decade, as the arsenal of aggressive states has grown richer. Also, in addition to cyber-attacks with technical effects, cyber-operations are often used for the purpose of information-psychological impact. In recent years, such cyber activities have gone beyond the area of post-Soviet countries, and European and US election processes have repeatedly become the target of hackers related to Russian government structures. Cyberspace has become an important arena for Russian propaganda content and Russian informational confrontation in general (Gotsiridze, 2019).

We have quite a lot of examples of attacks on critical infrastructure and general cyber warfare around the world. In most cases, the initiator of the attack is the Russian Federation, China, Iran and Nort Korea. In the 21st century, the Russian Federation is trying to influence various countries with both conventional war methods and elements of hybrid war. However, it should be noted that Georgia and Ukraine occupy the leading positions in the list of Russia's "victims". The Russian Federation is waging a full-scale war against Ukraine, and also uses all elements of hybrid war, including information warfare and cyber warfare. Russia launched its war on Ukraine on 24 February 2022, but Russian cyber-attacks against Ukraine have persisted ever since Russia's illegal annexation of Crimea in 2014, intensifying just before the 2022 invasion. Over this period, Ukraine's public, energy, media, financial, business and non-profit sectors have suffered the most. Since 24 February, limited Russian cyber-attacks have undermined the distribution of medicines, food and relief supplies. Their impact has ranged from preventing access to basic services to data theft and disinformation, including through deep fake technology (Przetacznik, Tarpova, 2022: 1).

The war in Ukraine started on different levels – on the ground and likewise in cyberspace. On 23 February, the day before Russia's invasion of Ukraine, cyberweapons became a prelude to all-out war. Computer systems in different Ukrainian ministries, government organisations, and banks were the targets of distributed denial of service (DDoS) attacks (Digital Watch, 2022: 1).

On February 24, at the same time as the start of the war, there was a cyber attack on the communication systems of the Kyiv post office and the KA-SAT satellite network. The mentioned attack caused communication interruption for individuals, public and private entities of Ukraine. On February 25, the IssacWiper cyber attack took place on government websites. On the same day, there was a cyber attack on the border control station. On February 28, cyber attacks were carried out on Ukraine's digital infrastructure (Przetacznik, Tarpova, 2022: 3–4). All this has led to blockage of financial access, disruption of services and disruption of energy resources.

On March 14, the CaddyWiper malware infiltrated the systems of several Ukrainian organizations. which affected both the government and financial sectors. Two days after this attack, a fake statement was broadcast on one of the Ukrainian TV channels, in which it was said that Volodymyr Zelensky was calling on the population to surrender.

Cyber-attacks against Ukraine from the end of March include phishing emails targeting the government and the military (17 March) and various organisations (18 March), as well as the use of a LoadEdge backdoor for installing surveillance software (20 March). Cyber-assaults targeting Ukrtelecom and WordPress sites caused a connectivity collapse and restricted access to financial and government websites (28 March). On 30 March, the MarsStealer information stealer accessed the user credentials of Ukrainian citizens and organisations (Przetacznik, Tarpova, 2022: 2).

Similarly, in April, hackers extracted sensitive information and user credentials from the Ukrainian government 2 and 7 April and media entities 7 April. They also seized citizens' banking and payment datawith the help of a Trojan malware 14 April and a fraudulentsocial media page survey 19 April. Other cyber-attacks sought to inflict societal harm. One such example included an attempt to hinder the activity of power stations and obstruct electricity flow to millions of people 8 April (Przetacznik, Tarpova, 2022: 2). Also, on April 22, a cyber attack took place on the Ukrainian post office, which produced stamps related to the war. On

May 7, cyber-attacks were launched to complement military operations, targeting government websites, telecommunication services and infrastructure. For instance, an attack aimed at the Odesa City Council occurred at the time of a missile attack on the city's residential zones. On May 9, hackers also launched a distributed denial-of-service (DDoS) attack on some of Ukraine's telecom operators to filter and re-route online traffic to occupied territories (Przetacznik, Tarpova, 2022: 4–5). But Ukraine's defences have held up relatively well, partly thanks to its experience going back years. Paul Chichester, the director of operations at the UK's National Cyber Security Centre describes the cyber-clash as "the most sustained set of cyber operations coming up against the best collective defence we have seen" (Corera, 2022).

Russian cyber attacks against systems in Ukraine, as part of the former's ongoing invasion attempt, have been almost entirely the work of government-backed intelligence and military agencies. This is according to a report from security vendor Trustwave, which said that known threat groups from the Russian Federal Security Service (FSB), Foreign Intelligence Service (SVR), and the Main Directorate of the General Staff of the Armed Forces (GRU) are responsible for the vast majority of attacks against both critical industrial infrastructure and data networks in Ukraine (Shaun, 2022). In a few cases, proxy groups (such as the leading ransomware group Conti) were also involved, and in one reported instance, a Brazilian hacker group supportive of Russia attacked Ukrainian universities (Lewis, 2022).

After the events of 2014, when Russia annexed Crimea, Ukraine actively started to develop cyber security. However, the introduction and development of the cyber defense system requires qualified specialists and huge finances, which Ukraine, unfortunately, did not have. In order for it to have better cyber defense systems, the support of NATO and the European Union was important in this regard. Over the past several years Ukraine's military and security services have purchased several different communications systems that run over Viasat's network, according to contracts posted on ProZorro, a Ukrainian transparency platform (Pearsin *et al.*, 2022). This is small compared to what the Ukrainian state needs, given its size and vulnerability. Ukraine has been actively developing its cyber security in recent years with the help of the European Union, NATO and the USA.

## The Russia-Ukraine war and NATO-EU cyber security policy

It should be noted that in the modern period, political, economic, energy, military, social and other processes have actively moved to the cyber space. Also, the shift of criminal processes to cyberspace has made cyber security one of the main segments of state security. Countries with strong cyber-offensive potential, and above all Russia, use their capabilities aggressively. Cyber attacks on Ukraine and Georgia are clear examples of all this. Russia successfully uses its capabilities both during war and conflict and in peacetime to gain geopolitical advantage. Consequently, there is never peace in the cyber domain, which has become the fifth domain of conflict, and its protection is very important for states. The Russia-Ukraine war that started on February 24, 2022 is a clear example of how Russia uses its advantage in cyberspace.

The Russia-Ukraine war is the largest conventional conflict of the 21st century, which is taking place using modern technologies and fighting methods. The hostilities that have developed since February 24, 2022 have shown that both the North Atlantic Treaty Alliance and its member and partner countries need to review their defense priorities and synchronize them with modern combat methods. All of this gives the belligerents an advantage over the enemy in hostilities in the contemporary world.

At the NATO Madrid summit, it was noted that Russia is actively using cyber attacks in addition to conventional weapons in order to gain an advantage over the opponent. In the ongoing Russia-Ukraine war, there have been quite a few cyber attacks on Ukrainian government institutions and critical infrastructure (Nye, 2022). Also, a cyber attack was carried out on the American company Space-X, which provided satellite support to Ukraine and gave a great advantage in the aspect of secure communication (Howell, 2022).

Since the beginning of the war in Ukraine, international organizations and leading states have been ready to help Ukraine in case of hybrid war risks. The US, NATO and the European Union have activated cyber security mechanisms. The main objective was to protect the basic critical infrastructure. The European Union has activated cyber security rapid response teams within the framework of the Permanent Structured Cooperation (PESCO) project. It should be noted that counter-attacks were carried out by private hackers on the Russian state security, banking and media systems.

The operation targeting KA-SAT – resulting in communication outages for individuals and public and private Ukrainian entities was condemned by the EU High Representative (HR) on 10 May. The HR described it as ‘another example of Russia’s continued pattern of irresponsible behaviour in cyberspace’, adding that cyber-attacks targeting Ukraine ‘could spill over into other countries and cause systemic effects putting the security of Europe’s citizens at risk’ (Przetacznik, Tarpova, 2022: 1).

NATO, of course, is actively involved in Ukraine’s cyber security processes. But in this regard, the policy of the alliance is still cautious, like that of other states and international organizations. The caution stems from the fact that in some way the war does not escalate and involve other countries. Russia is trying to intimidate various European states into not helping Ukraine fight cyber threats.

It must be said that for more than 70 years, NATO has been developing its technologies to ensure the protection of allies and member states. In February 2021, the Alliance's defense ministers approved a strategy on emerging and disruptive technologies. NATO is cooperating with the European Union and the United Nations in the direction of developing and damaging technologies to fully solve the problems.

The NATO has many challenges in this direction integrating cyber into joint functions and warfighting is one of the important issues for success. NATO must have a clear vision of where it is going and what it wants to achieve. In fact, cyber technologies should have a greater role in joint operations.

Also, compliance with standards is really one of the most important issues in the direction of cyber security and information security. It should be noted that NATO works quite well in this direction. NATO is helping Ukraine and Georgia to strengthen their cyber security and defense capabilities. These two states, as they get closer to NATO standards in terms of cyber security policy, will be able to repel cyber attacks coming from Russia and other states much more easily.

In the North Atlantic Alliance, there is a standardization office (NSO – NATO Standardization Office), which has placed the issue of cyber security in advanced positions. The above organization coordinates, supports and manages NATO's standardization activities.

New strategy: In a new strategy document, NATO reaffirmed a 2021 commitment that a cyberattack could (but would not automatically) trigger Article 5 of the North Atlantic Treaty, which would make it an attack against the alliance as a whole. It also pledged to work with the private sector to counter threats, formally recognized threats in cyberspace posed by Russia and China, and promised to update NATO's command structure to reflect new cyber threats. Also in the new strategy of NATO's will include over $1 billion to fund research into emerging technologies including quantum computing and artificial intelligence (Maggie, 2022).

It should be noted that a modern force, as well as, for example, an innovative defense technology international organization, must be able to use, store, secure, analyze and share large amounts of data from anywhere.

Also, governments are starting to realize how important cyber security really is. The actuality and seriousness of the mentioned issue have been shown to us by the events in Ukraine, as well as by the cyber attacks on other countries, including Georgia.

The first country in the world (in terms of cyber technologies) is the United States of America. It provides significant assistance to Ukraine in this difficult period. The finances of this state in the direction of cyber security are colossally high – every year it increases funds for the development of cyber capabilities. In March 2022, President Biden's administration released its fiscal 2023 budget, which earmarked $11 billion toward civilian cybersecurity spending, an 11% increase from the year before (Jones, 2022).

In 2009, in the United States of America, the Cyber Command (CYBERCOM) was established, which represents the unified combat command, it is the highest division in the army of this country. They can be assumed to have contributed to activities such as retaliatory cyber attacks against the Islamic State of Iran and the Russian Federation. It is impossible to say precisely at this stage, but there is an assumption that the Islamic State of Iran is also helping Russia in conducting cyber war against Ukraine. This is already a matter of investigation and probably the US special services will investigate.

## Conclusion

Cyber security is a global challenge that transcends national borders and requires increased cooperation at the international level. Therefore, the new cyber security strategy of Ukraine and Georgia should be based on modern standards. Take into account the best practices of partner countries, which is one of the main principles of collective defense. Also – to ensure compatibility with EU, NATO and Alliance member states in the field of cyber defense. In the context of global security, timely prevention of threats and deepening of cooperation with partner states and organizations is important for Ukraine.

Despite the fact that the Russia-Ukraine war has changed many things (Russia-China relations have strengthened, drones have proven their effectiveness in warfare, the world has returned to the policy of nuclear intimidation, the war has caused a global food crisis, an energy crisis in Europe, the architecture of international security has changed, the process of establishing a new world order is underway, etc.) in today's world, at least one issue has not been removed from the agenda – along with the development of cyber technologies, cyber defense systems and programs must be improved and developed. Also, the joint cooperation strategy should be refined.

It is true that cyberspace has become an integral part of modern warfare. However, it should be noted that it was not of critical importance in the Russia-Ukraine conflict. Accordingly, for both NATO and its member and partner countries, strengthening the defense capabilities for traditional warfare should be a high priority direction. In war, states have to use all the resources at their disposal, which in many cases do not directly depend on cyberspace. The ongoing Russia-Ukraine war shows that hard power remains a mechanism for realizing Russia's imperialist goals. And modern fighting methods require constant adaptation from sovereign states. Based on the above, Ukraine and Georgia, together with NATO and its member and partner countries, should try their best to strengthen their defense capabilities and approach by observing and analyzing the current Russia-Ukraine military operations.

## Bibliography

Asaro, P. 2020. 7 *Autonomous Weapons and the Ethics of Artificial Intelligence*, p. 1, https://academic.oup.com/book/33540/chapter-abstract/287905547?redirectedFrom=fulltext&login=false (accessed 18.11.2022).

Corera, G. 2022. Ukraine war: Don't underestimate Russia cyber-threat, warns US. *BBC News*, p. 1, https://www.bbc.com/news/technology-61416320 (accessed 27.08.2022).

Digital Watch. 2022. *Ukraine conflict: Digital and cyber aspects*, p. 1, https://dig.watch/trends/ukraine-conflict-digital-and-cyber-aspects (accessed 22.08.2022).

Duić, I., Cvrtila, V., Ivanjko, T., 2017. *International cyber security challenges*. University of Applied Sciences Vern, Zagreb, Croatia, MIPRO. https://doi.org/10.23919/MIPRO.2017.7973625

Foley, J. 2022. *FBI Reveals Alarming Rise in Cost of Cyberattacks*, p. 1, https://www.mimecast.com/blog/fbi-reveals-alarming-rise-in-cost-of-cyberattacks/ (accessed 20.09.2022).

Gotsiridze, A. 2019. *Cyber Security Strategy and Key Challenges*, p. 1, https://1tv.ge/video/kiberusafrtkhoebis-strategia-da-mtavari-gamowvevebi/ (accessed 11.08.2022).

Howell, E. 2022. *Elon Musk says Russia is ramping up cyberattacks on SpaceX's Starlink systems in Ukraine*, p. 1, https://www.space.com/starlink-russian-cyberattacks-ramp-up-efforts-elon-musk (accessed 20.09.2022).

Jones, D. 2022. Biden administration's FY 2023 budget includes 11% increase for cyber. *Cybersecurity Dive*, p. 1, https://www.cybersecuritydive.com/news/biden-2023-budget-cybersecurity/621264/#:~:text=The%20budget%20earmarks%20%242.5%20billion,after%20Congress%20appropriated%20additional%20funding (accessed 12.09.2022).

Lewis, J.A. 2022. *Cyber War and Ukraine*, Center for Strategic and International Studies, p. 1, https://www.csis.org/analysis/cyber-war-and-ukraine (accessed 27.09.2022).

Maggie. M. 2022. NATO establishes program to coordinate rapid response to cyberattacks. *Politico*, p. 1, https://www.politico.com (accessed 15.08.2022).

Nye, J., S. JR,. 2022. *Eight lessons from the Ukraine War*, p. 1, https://www.project-syndicate.org/commentary/russia-war-in-ukraine-eight-lessons-by-joseph-s-nye-2022-06?barrier=accesspaylog (accessed 8.09.2022).

Pearson, J., Satter, R., Bing, C., Schectman. J. 2022. *Exclusive: U.S. spy agency probes sabotage of satellite internet during Russian invasion, sources say*, p. 1, https://www.reuters.com/world/europe/exclusive-us-spy-agency-probes-sabotage-satellite-internet-during-russian-2022-03-11/ (accessed 21.08.2022).

Przetacznik J., Tarpova, S. 2022. *Russia's war on Ukraine: Timeline of cyber-attacks*, EPRS. European Parliamentary Research Service, PE 733.549, pp. 3–7, https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI(2022)733549_EN.pdf (accessed 18.09.2022).

Shaun, N. 2022. *Russian cyber attacks on Ukraine driven by government groups*, p. 1, https://www.techtarget.com/searchsecurity/news/252523950/Russian-cyber-attacks-on-Ukraine-driven-by-government-groups (accessed 24.08.2022).