Історико-політичні проблеми сучасного світу:
Збірник наукових статей. – Чернівці:
Чернівецький національний університет,
2019. – Т. 40. – С. 50-57
DOI: 10.31861/mhpi2019.40.50-57

Modern Historical and Political Issues:
Journal in Historical & Political Sciences. – Chernivtsi:
Chernivtsi National University,
2019. – Volume. 40. – pp. 50-57
DOI: 10.31861/mhpi2019.40.50-57

**УДК: 327.88:004]:327.54**

**© Alika Guchua[1]**
**© Thornike Zedelashvili[2]**

## Cyberwar as a Phenomenon of Asymmetric Threat and Cyber-Nuclear Security Threats

The work deals with the topic of cyberwar as a phenomenon of asymmetric threat and cyber-nuclear security threats in modern world politics, potential threats to international politics and global security issues, counter-terrorism policies are discussed. The paper discusses the challenges facing cyber security worldwide and the phenomenon of cyber security against the backdrop of asymmetric threats. Cyberspace has already become a weapon of infinite capacity for the whole world. It has generated positive effect as well as has become the area of evil for terrorists, which are actively using modern technologies, computer systems. The facts are many and we are often in the center of events. With the development of technology in the 21st century, global changes are taking place in international security, the geopolitical transition and new threats and challenges, and international security issues are becoming increasingly important. The international security system is vulnerable to challenges such as the use of weapons of mass destruction and cyber terrorism. The article discusses the dangers and problems of hybrid warfare in international security, as well as the Russian-Georgian hybrid warfare.

**Keywords:** Cyberwar, asymmetric threat, hackers, attack, hybrid war, Russia-Georgia, NATO, EU, nuclear terrorism, nuclear security.

## Кібервійна як феномен асиметричних загроз та загроз кіберядерній безпеці

У статті розглянуто тему кібервійни як явища асиметричної загрози, загрози кіберядерній безпеці в сучасній світовій політиці. Нині кібервійни є потенційною загрозою для процесу міжнародної політики та глобальної безпеки. Проаналізовано проблеми, що стоять перед кібербезпекою у всьому світі та стан кібербезпеки. Вони розглядаються на тлі асиметричних загроз, а тому досліджено і антитерористичну політику. Продемонстровано, що кіберпростір вже став зоною безмежних можливостей для зловмисників всього світу. Попри позитивний ефект використання інтернету, існують небезпідставні уявлення про кіберпростір як зону зла для терористів, які активно працюють використовуючи сучасні технології та комп’ютерні системи. З розвитком технологій у XXI столітті, в міжнародних відносинах відбуваються глобальні геополітичні зміни, з’являються нові загрози та виклики міжнародній безпеці, а тому питання асиметричних загроз та загроз кіберядерній безпеці стає дедалі важливішим.

Усі держави вразливі перед такими викликами, як використання зброї масового знищення та кібертероризму. У статті розглядаються небезпеки та проблеми гібридної війни в міжнародній безпеці, а також російсько-грузинська гібридна війна.

**Ключові слова**: кібервійна, асиметрична загроза, хакери, атака, гібридна війна, Росія-Грузія, НАТО, ЄС, ядерний тероризм, ядерна безпека.

**Main players of the cyberspace and 2008 Russia-Georgia cyber war.** In modern times, in the global processes of the world cyberspace plays an important role as a phenomenon of struggle and a new political conflict area. Ensuring international security is most relevant at the level of national security, on the background of new threats and challenges. One of the key and main issues in global

[1] Ph.D student, assistant Head of the MA Program in International Relations and International Security Studies, Faculty of Social Sciences, Caucasus International University, Georgia. E-mail: alikaguchua7@gmail.com,; https://orcid.org/0000-0003-0347-9574.

[2] Ph.D student, Faculty of Social Sciences, Caucasus International University, Founder Information and analytical agency “Leader”, Georgia. E-mail: thomas_zedelashvili@mail.ru; https://orcid.org/0000-0003-2630-1779.

politics is the new dimensions of political conflicts. Cyber-attack, information war, as part of the "hybrid war", are important as to determine the course and the essence of the unfolding of the processes of international security.

Cybernetic space creates many hazardous conditions, not only on the national level, but also on a global scale, cyber-attacks in today's reality accompany all military conflicts that are taking place around us. For example, we can discuss the Russian-Estonian cyber-war in 2007, the cause of which was the initiative of Estonian people and government regarding the transferring the Soviet Memorial Monument of the Second World War elsewhere. The second and quite widespread and diverse war occurred between Russia and Georgia in 2008. During this war, along with military intervention, cyber-attacks took place on the websites of state agencies and news agencies of Russia, which resulted in malfunctioning of almost all state and information web sites. On August 9, all Georgian domains were no longer searchable. When going to the website of the Ministry of Foreign Affairs of Georgia the pictures of President Mikheil Saakashvili and Hitler appeared[3]. This information is also reflected in the report of the Ministry of Foreign Affairs in 2009.

It is noteworthy that Georgian intelligence and counter-intelligence agencies in this direction, along with all other things, were not able to respond and have suffered a complete collapse. When the hacker attacks took place on the web sites, Georgian state agencies tried to create alternate blogs and thus inform the population in cybernetic space, but these blogs were actively attacked and blocked.

It is also worth mentioning the Russian-Ukrainian war, where almost every elements of the "hybrid war" has been used, including the most intense cyber and information attacks.

If we look back to the past few years, we can say that together with the change and development of the cybernetic space, the cyber wars have changed and has also developed. The ongoing processes in the world should be taken into consideration, because even the superpower, like the United States, cannot defend itself from cyber-attacks. For example, the US presidential election in 2016 between Hillary Clinton and Donald Trump, where there was a doubt that Russia's involvement in this election was through hacker attacks. While the US investigation has already completed the case study and made an official statement, that Russia did not contribute to Trump's presidency, but it was also said that there was an obvious attempt. If there was an attempt, perhaps Donald Trump will finish his presidential career so that he will never get rid of this rumor. In this case, we go back to the topics of the fake news and social networks.

Different social networks are actively used in cybernetic space, which also represents one of the most threatening events. The primary goal and objective of the social network was that one person in the university could easily contact others, boys would have simple contact with girls, but the virtual space went beyond all borders and transformed into a kind of a space for information, advertising, misinformation, psychological terror. One of the most powerful mechanisms of warfare, which has always existed in different ways in world history, is actively used in cybernetic space – the most dangerous component – misinformation. Intelligence and counter-intelligence agencies have used this method more intensively both now and in the past. Misinformation in a global scale, as well as in Georgia is a part of daily life that effectively influences the lower class of the population. During the 2018 presidential election, many disinformation spread by political parties on opponents and various issues. One of the misinformation was that such a hacker interference occurred from the Russian side in the elections, which was an absolute absurd. However, on the masses, on people have no access to the computer and were not able to catch up with the technological development, it has worked effectively. This misinformation was, of course, coming from the United Opposition forces and, in particular, the "National Movement". As for the interference of Russia through the hackers in the presidential election, it would not have been possible because elections were not carried out by electronic system. However, Russia's involvement was obvious on the other hand when Vitaly Shliarov's team, a group that was warmly welcomed at Vladimer Putin's door, headed the PR campaign of the presidential candidate of united opposition, Grigol Vashadze. This is the Vitaly, who helped Ksenia Sobchak's PR campaign as a consultant in last presidential election in Russia. After the election, it became clear that this oppositional move was made by Ksenia Sobchak, was planned by Vladimir Putin.

[3] Markof J. "Before the Gunfire, Cyberattacks", "The New York Times", USA, Aug. 12, 2008 year, page 1, URL: http://nytimes.com.

Questions arise during research: what preconditions proceed the initiation of cyberwar and under what circumstances it originated as one of the terrible species of crime, how the stages passed, and what stage is it on currently? Today humanity does not have the right to take it easy – the more modern and future technologies develop (and will surely develop), the terrorists will cause the more danger. Technologies improve? The methods of cyber, terrorist and information warfare also improve. There is an impression that "the fathers of terrorism" achieve such peaks, that are even ahead of technology development and scientists are forced to follow the so-called Achievements, i.e., invent defensive methods. This is an ordinary war, scientists are studying "achievements" of terrorists and terrorists study the achievements of scientists. That is how it was, how it is today and so will be in the future, the main thing for humanity is that science should not stay far behind the activities of practicing murderers. While researching this topic**, cyber-war as a phenomenon must be divided into several directions: first – technological war or use of techniques; the second is the theory, i.e., the processing and use of propaganda methods; third – the use of all this in practice,** i.e. what is the result. We should look at any event from the two sides, one is when you fight against terrorism, you carry out real war in the Internet space, and the second is how are you, as a humanity, are attacked , what methods are used by the servants of evil. If you do not look at the event from the other side, if you do not make a diagnosis and do not make a serious analyze, then you will lose any war – technological, theoretical and practical. Here arises a question: What is the situation now, whether humanity loses the fight against evil? Analysis of the past years shows that it is not losing, and neither does it win to zero. Let us look at the series of terrorist attacks in the United States or in Western Europe, even in Afghanistan, Syria and Iraq, in this respect today's world has lot of troubles. Even if we recall the September 11, 2001, the 19 Islamist terrorist skyjacked four commercial passenger aircrafts. The skyjackers intentionally targeted two planes in New York at the two skyscrapers of World Trade Center (so-called twins), resulting in death of all passengers and a large number of the people in those buildings. Both buildings collapsed for two hours, and took along the surrounding two buildings, and many more were damaged. The skyjackers crushed the third plane into the Pentagon building. The fourth plane fell onto the Valley of Somerset-Kent (Pennsylvania). All passengers of the four airplanes were killed. This is a practical war that was preceded by cyber and propagandist wars. Perhaps no one could imagine such results, no one could imagine if such sacrifices would be caused by the evil established in the world, but this fact showed us that if the terrorists had the power, they would start a Third World War with no doubt. Did the super state turn out to be powerless against terrorism? Yes, it turned out to be so. Everyone thought that the most secure and safe country was the United States, it turned out to be a wrong assumption. If anyone thinks that Islamists have just sneaked into the airplane and then crashed onto the ground, is being very mistaken. Of course, this was accompanied with a serious preliminary work in order for the terrorists to fulfill their intentions. The world's leading lawyers have already investigated all four cases, all of the four cases (separately) are filmed and all the details are fully restored. In order to cross the barriers of the airports and to get in the airplane with guns, it needs computer processing at the scientific level. Despite the fact that a long time has passed after the terrorist act, it is the subject of consideration and instructive case for the specialists. Although the red line of terrorism currently goes on the Muslim countries and the fanatic groups are prepared in these countries, specialists still acknowledge that Russia has the most serious experience of conducting propaganda war worldwide.

Cyber element today is an important component of all wars and conflicts. For Georgia as for a permanent object of the Russian interest, protection of cyberspace should be recognized as a priority direction for defending its national security and ensuring defense. Sandro Gotsiridze, expert in cyber security says in his work ("the cyber aspects of the post-Soviet conflicts and Georgia – using cyber elements in modern conflicts"), that it is important to consider the latest trends of using cyber elements in war or crisis situations:

"Cyberspace, as the area of confrontation of parties, gains more value every day. The number of units/divisions involved in the cyber security sphere of developed countries is increasing daily, and the budget is equal to billions of dollars"[4].

[4] Gotsiridze S. "Cyber-attack becomes a method of conventional combat", Tbilisi, 2010, p. 1, URL: https://www.radiotavisupleba.ge.

According to Sandro Gotsiridze, a different form of cyber element accompanied the majority of active combatting confrontations of the last period. The cyber confrontation characterized the Libyan war, partly the Syrian conflict, and cyber espionage and cyber warfare is the constant background of the international relations. The Stuxnet episode, discovery of the spy virus or networks (Duqu, Flame, Gauss, Miniduke, Red October, Wiper) – the cyber espionage or diversions, this incomplete list increases day and night from the end of the first decade of the 21st century and gains more significance.

**Cyber security policy and hybrid war.** When we talk about "hybrid wars", cyber wars, information wars and their constituents, security and discuss this issue from the different points of view, we should highlight and focus on approaches and positions of the North Atlantic Alliance. In the context of security, NATO is the world's most powerful organization, capable of resisting both the technological as well as the physical and financial resources to prevent the threats coming from the world. Active work is underway in the North Atlantic Alliance regarding the defensive issues of hybrid wars and it is visible in the ongoing processes. We can say that after the Warsaw Summit in 2016, NATO has undertaken fundamental reforms and is actively cooperating with partner countries in terms of cyber security.

From the example of Georgia, we can say that since 2010 "Caucasus Academy of Security Experts" (CASE) functions, which trains and retrains the military, law enforcement, diplomats, large corporations and students.

Since 2012, the Ministry of Education, Science, Culture and Sport of Georgia has launched the Cyber Security School[5] in Georgia, where anyone can retrain.

In May 2013, the President of Georgia signed the Cyber Security Strategy[6] for 2013-2014, which is the main document that defines the state policy on cyber security.

On February 6, 2014, the LEPL Cyber Security Bureau[7] was established based on the Decree No. 8 of the Minister of Defense of Georgia and its Charter was approved.

"Cyber Security Association"[8] is also functioning in Georgia, which carries out trainings and retraining in cyber security.

From the point of view of our research topic, it is noteworthy to mention new geostrategic tasks of NATO, at present, the military-political organization NATO has activated an appropriate plan, through which joint activities are planned with partner countries and organizations, which, of course, is associated with the improvement of security environment of Georgia.

As for the "hybrid war", diplomatic, informational, economic and military, these are the basic tools of the "hybrid war", using which one state carries out hostile actions against another to achieve its own interests. The clearest example of this is Ukraine, where the Russian Federation is trying to keep its influence using all these elements. In modern "hybrid wars", new elements have been identified – economic, cyber-attacks, nuclear threats, information wars. The most striking example of nuclear threat is the expressions of Russian diplomats against the sovereign choice of Sweden and Finland.

Czech Deputy Foreign Minister Ivan Jestrab said that during the "hybrid war", the main advantage has the aggressor, because the effect of the unexpectedness is large and the borders are demolished[9].

In the North Atlantic Alliance, the "hybrid war" is called tactics after the Warsaw Summit it become clear that NATO has made unprecedented steps for the post-cold period, they have chosen the direction towards the adaptation of the Alliance with the new security environment, and NATO is always ready to protect its Member States, from any thrats coming from any direction.

As former NATO advisor on security issues, General Frank Van Kappen notes: "To prevent and overcome international threats, it is necessary for the States to create a united strategic approach in many directions and, of course, to carry out coordinated actions"[10].

[5] Ministry of Education, Science, Culture and Sport of Georgia, Tbilisi, 2012, p. 1, URL: http://mes.gov.ge.

[6] Ministry of Internal Affairs of Georgia, "Legislation on cybercrime and general policy", Tbilisi, 2013, p. 1, URL: http://police.ge.

[7] LEPL "Cyber Security Bureau", Charter, Tbilisi, 2014, p. 1, URL: http://csbd.gov.ge.

[8] Cyber Security Association, Tbilisi, 2017, p. 1, URL: http://scsa.ge.

[9] Jestřáb I. "Hybrid war and its influence on NATO member and partner countries", Tbilisi, 27 Oct. 2015, p.1, URL: http://mod.gov.ge.

[10] Artyukh V. "Fog of the "Hybrid War": why it is harmful to think hibridally", Russia, 30 September, 2016, p. 1. URL: http://september.media/archives/294.

In this regard, the interview of the famous political scientist Soso Tsintsadze is interesting. He told us that the era of the Information War begins with the enhanced methods after the end of the "cold war", which was baptized as a "hybrid war":

"With the development of social networks, almost unlimited resources for informational war producers are created. "Attraction" of the information war consists in the difficulty of defense against it. Hackers are already involved in elections, but it is difficult to prove particular cases. What we see today, in our view, is the beginning; the future will be more intense, because already lot of money is spent on this issue.

For example, Russia spends billions in order to gain influence in all areas, especially from political point of view"[11].

**Asymmetrical threats and jihadist cyber war.** In the 2018 report published by the State Security Service of Georgia, more details are presented on what is jihadist cyber war and what kind of danger we may face.

In 2018, for Georgia, as well as for many other countries, the main challenge was the terrorist organization "Islamic State" ("Daesh") and groups related with it. "Daesh" continued to act with a new strategy developed after weakening and loss of territories. Within the framework of this, it was no longer a priority for "Daesh" to mobilize supporters in Syria and Iraq. The main weapon of the terrorist organization became carrying out terrorist acts beyond the conflict zone. "Daesh" urged radicalized people residing in different countries around the world to carry out terrorist attacks by any means. The terrorist organization has been actively disseminating its own ideology, using modern technologies, including the Internet and social networks, to radicalize and recruit individuals.

As we read in the report: Al-Qaeda operated mainly through regional groups operating in the Middle East and African continent. The Taliban continued to attack Afghan government forces and the military of the international mission in Afghanistan.

Professor Vakhtang Maisaia conducted a thorough research of this topic. In his work, it is clear what Islamis State – "Daesh" and "Al-Qaeda" represent:

"These are terrorist organizations that are inspired by the idea of creating a united Islamic Caliphate in the Middle East. However, together with the events in the region, with the use of mass media and global information networks, Islamic extremist and radical ideas and the fulfillment of these ideas have long ago crossed the borders of the combat grounds. This was possible to achieve by the use of a wide range of Internet resources by the terrorists, and with the rapid spread of their ideas via Internet"[12].

Jihadist networks are created daily in a variety of forms. Here goes, so to say, selective work to bring up new generation jihadists. As Vakhtang Maisaia says, these are the second and third generation jihadists, who have to work "in the back of the enemy".

Today more than 10 thousand web sites operate in cyberspace, through which jihadist ideology and practice of terrorism is disseminated. If we add more than 10 thousand web sites to a wide variety of social networks, we will get a very big danger that needs resistance that is more powerful. This cannot be done individually, under the supervision of one country, even if this country is a super-state. In this case, unprecedented cooperation and working on new technologies are needed. One of the main challenges for modern world security is asymmetric threats such as international terrorism and transnational organized crime. Weapons, including weapons of mass destruction and its constituents. As well as drug trafficking and trade, human trafficking and cybercrime.

**Cyber-nuclear security threats.** Nuclear weapons systems were developed before the advancement of computer technology and little consideration was given to potential cyber vulnerabilities. As a result, current nuclear strategy often overlooks the widespread use of digital technology in nuclear systems. Nuclear weapons systems are at threat from hostile states, criminal groups and terrorist organisations exploiting cyber vulnerabities. The likelihood of attempted cyber-attacks on nuclear weapons systems is relatively high and increasing from advanced persistent threats from states and non-state

[11] Tsintsadze S. "Strategy of the informational war and new geostrategic tasks of NATO", Master's Thesis of Tornike Zedelashvili, "Caucasus International University" Tbilisi, 2017, p. 11.

[12] Maisaia V. "Specifics of the informational-propagandist / cyber-virtual war of the "Islamic Caliphate" – concepts of the "soft power", Tbilisi, 7 Jan. 2017, p. 1. URL: http://geotimes.ge.

groups. The US could have infiltrated the supply chain of North Korea's missile system that contributed to a test failure in April last year. The silos of US nuclear-tipped Minuteman intercontinental ballistic missiles "are believed to be particularly vulnerable to cyber attacks". [13] The group in Belgium affiliated to Islamic State monitoring the movements of a nuclear scientist; and German-owned Patriot missiles reported to have been hacked in 2015.

In the context of ongoing geopolitical changes in the modern world, NATO faces new risks and challenges in the world. The new challenges of the Alliance are threats from the eastern and southern flanks, and the current situation has prompted NATO to develop a new military-strategic concept to ensure complete security and ensure the stability of the future alliance. Due to the nuclear threat, the need to change NATO's military strategy is being actively discussed. NATO Secretary General Jens Stoltenberg says NATO will adopt a new strategy. At the same time, he emphasized Russia's occupation of the Crimean peninsula after 2014 and its subsequent annexation. He said the cause was new NATO challenges and the nuclear threat from Russia. According to Stoltenberg „This Cold War era military alliance is revitalizing itself – already embroiled in Afghanistan, it's now talking up a fresh start in its relations with Russia as it unveils a new strategic plan to cope with a new range of threats including cyber terrorism"[14].

It is likely that the new NATO strategy will be based on a policy of non-use and timely containment of Russia's opposition. A nuclear deterrence policy and a Nuclear Planning Committee will be created along with elements that existed during the Cold War. So-called Russia was introduced in 2015. According to the Gerasimov doctrine, Russia decided that it would use nuclear weapons first. Given the current situation, NATO must take countermeasures. NATO must balance Russia's countermeasures to deploy strategic offensive weapons and nuclear missile systems, including nuclear warheads. The new strategy covers four main areas: a) strengthening positions in the Black Sea; b) the fight against cyber terrorism and cyber threats; c) increasing the impact on Moscow through sanctions and unification; And (d) a package of assistance to allied states. NATO's strategic concepts have been adapted to the threats and challenges facing the Alliance. With all this in mind, it can be argued that NATO's strategic concepts, given the time available, have responded to the threats and challenges that the Alliance faces.

Governments need to address the problems that can be created by cyber capabilities. To avoid this problem first step is develop a better understanding of the threat, including by answering the following questions: Its very interesting what are the feasible targets within the entire contribute chain, the nuclear weapons system itself and within the reform, modernization and maintenance processes? What kind of vulnerabilities do they have? Moreover who are the potential actors likely to carry through a serious cyber attacks? And which state, non-state actor or state-sponsored group would have an interest and the resources and capabilities?

All states which have nuclear weapons, hosting NATO nuclear weapons on their soil, or running a civil nuclear program should conduct annual assessments of the cyber resilience of all systems in question. It is very important to improved information sharing on possible and actual vulnerabilities and lessons learned with the biggest technology companies, vendors and manufacturers, suppliers, because will Introduce international security standards. These companies not keen to release of information, because their information is not used by hackers and competitors. It's important Government and business work closely together that solve all problems that are related to cyber attacks.

It is also important to consider the dangers and risks associated with nuclear safety. Communications as well as the transfer and storage of data are key targets for cyberattackers. In an earlier United Nations Institute for Disarmament Research (UNIDIR) paper, the International Security Department at Chatham House identified several areas within nuclear weapons systems that could be potentially vulnerable to cyberattacks[15]:

[13] Cyber-attack risk on nuclear weapons systems 'relatively high' – thinktank. 11 Jan 2018. p. 1. https://www.theguardian.com/technology/2018/jan/11/cyber-attack-risk-on-nuclear-weapons-systems-relatively-high-thinktank.

[14] Nato's Secretary General, Anders Fogh Rasmussen. Pg.1. URL: https://www.bbc.co.uk/programmes/p00cbjln.

[15] Beyza Unal and Patricia Lewis, „Cybersecurity of Nuclear Weapons Systems Threats, Vulnerabilities and Consequences", International Security Department, January 2018. Pg.5. URL: https://www.chathamhouse.org/sites/default/files/publications/research/2018-01-11-cybersecurity-nuclear-weapons-unal-lewis-final.pdf.

- Communications between command and control centres;
- Communications from command stations to missile platforms and missiles;
- Telemetry data from missiles to ground- and space-based command and control assets;
- Analytical centres for gathering and interpreting long-term and real-time intelligence;
- Cyber technologies in transport;
- Cyber technologies in laboratories and assembly facilities;
- Pre-launch targeting information for upload;
- Real-time targeting information from space-based systems including positional, navigational and timing data from global navigational systems;
- Real-time weather information from space-, air-, and ground-based sensors;
- Positioning data for launch platforms (e.g. submarines);
- Real-time targeting information from ground stations;
- Communications between allied command centres; and
- Robotic autonomous systems within the strategic infrastructure[16].

Subject to exploitation by groups or individuals with malicious intent are these areas. In the analysis, as the attack surface (the number of vulnerabilities in the system or network) increases, and if the security measures are canceled, malicious cyber attacks will increase. For each and every cognitive of nuclear weapons systems, there are various ways, also known as attack vectors, through which the malicious actor could access sensitive information and even create phishing information. These attack vectors include the use of remote malware, pre-installed exploits, or access systems before activating human elements.

The interaction between cyber operations and nuclear weapons is a complex problem. The complexity and danger of interaction is only partly a function of technology, but also a function of significant political, economic and strategic differences associated with the use of cyber and nuclear potential. Therefore, international organizations and the participation of states in nuclear safety are important and necessary.

**Conclusions.** Cyber war, asymmetric threat, use of internet space in terms of terrorism. This is the basic red line and the content of the paper. In addition, it is a subject of research as to what serious problems or threats the civilized world faces. What positive results has the technology development and at the same time, what challenges appear every day? This is the moment when no one should care for themselves only, how are we to be involved in the international defense system, not to become a victim of terrorism, as many countries have become? Today, the only guarantee of stability is the Western course and realizing all the challenges that concerns the modern world. Georgia is on a right way in these terms. However, we still need a lot of work to become a full member of this world.

Preventive measures. Since Georgia is located on the crossroads of Europe-Asia and represents a transit corridor for terrorists or drug traffickers, naturally their interest is present here too. State structures have already recognized that there are groups of persons with extremist opinions in the country, the aims of which are not at this stage, the conflict with the state. It is not excluded that in the future they might use their own connections and financial opportunities in favor of various extremist or terrorist groups or organizations. Extremism often changes its form and changes into terrorism, which is associated with the hybrid war, which implies the information and ideological war itself. The only thing that will confront all this is preventive measures taken by the state.

It is imperative that states agree with each other on the proliferation and security of weapons of mass destruction, for example: possible smuggling, cross-border criminal activity, nuclear material, to prevent the illegal transport of radioactive substances and components of weapons of mass destruction. We are on the verge of a completely different global nuclear order, where the problems of nuclear weapon control will change.

Cyber vulnerabilities in nuclear weapons systems and structures pose a range of dangers and risks. At best, cybersecurity in nuclear weapons systems can undermine trust and confidence in military capabilities and nuclear weapons infrastructure. In the worst case, cyber attacks can lead to deliberate misinformation and unintentional launch of nuclear weapons. In times of crisis, the loss of confidence

[16] Beyza Unal and Patricia Lewis, Op. cit.

in the potential of nuclear weapons can affect decision-making and can undermine confidence in nuclear deterrence, especially in expanding nuclear deterrence for allied countries. The challenges that cyber risks pose to nuclear weapons systems can be seen as the possibility of creating an end-to-end risk reduction measure that benefits both traditional proponents and skeptics of nuclear deterrence.

The registration and protection of nuclear materials is a global issue. Putting them in the hands of terrorists and criminals is a big threat to everyone. Governments and decision makers in nuclear-weapon states should also publicly acknowledge that cybersecurity for nuclear weapons systems is a top priority for the security of national military programs. In the modern world, it is difficult to determine the level of threats, so it is important to pay close attention to the protection of nuclear facilities in the world. When it comes to the safety of nuclear weapons, this not only reduces its credibility and deterrent value, but also poses a huge threat to security. Nuclear safety is a very complex issue, so it needs to be studied in more detail.

## References

1. Artyukh V. “Fog of the “Hybrid War”: why it is harmful to think hibridally”, Russia, 30 September 2016, URL: http://september.media/archives/294.
2. Beyza Unal and Patricia Lewis, “Cybersecurity of Nuclear Weapons Systems Threats, Vulnerabilities and Consequences”, International Security Department, January 2018. URL: https://www.chathamhouse.org/sites/default/files/publications/research/2018-01-11-cybersecurity-nuclear-weapons-unal-lewis-final.pdf.
3. Cyber Security Association, Tbilisi, 2017, URL: http://scsa.ge.
4. Cyber-attack risk on nuclear weapons systems “relatively high” – thinktank. 11 Jan 2018. URL: https://www.theguardian.com/technology/2018/jan/11/cyber-attack-risk-on-nuclear-weapons-systems-relatively-high-thinktank.
5. Gotsiridze S. “Cyber-attack becomes a method of conventional combat”, Tbilisi, 2010, URL: https://www.radiotavisupleba.ge.
6. Jestřáb I. “Hybrid war and its influence on NATO member and partner countries”, Tbilisi, 27 Oct. 2015, URL: http://mod.gov.ge.
7. LEPL “Cyber Security Bureau”, Charter, Tbilisi, 2014, URL: http://csbd.gov.ge.
8. Maisaia V. “Specifics of the informational-propagandist / cyber-virtual war of the “Islamic Caliphate” – concepts of the “soft power”, Tbilisi, 7 Jan. 2017, URL: http://geotimes.ge.
9. Markof J. “Before the Gunfire, Cyberattacks”, “The New York Times”, USA, Aug. 12, 2008 year, URL: http://nytimes.com.
10. Ministry of Education, Science, Culture and Sport of Georgia, Tbilisi, 2012, URL: http://mes.gov.ge.
11. Ministry of Internal Affairs of Georgia, “Legislation on cybercrime and general policy”, Tbilisi, 2013, URL: http://police.ge.
12. Nato’s Secretary General, Anders Fogh Rasmussen. URL: https://www.bbc.co.uk/programmes/p00cbjln.
13. Pataraia L. “Caucasus Academy of Security Experts”, Tbilisi, 2010, http://globalcase.org.
14. Tsintsadze S. “Strategy of the informational war and new geostrategic tasks of NATO”, Master’s Thesis of Tornike Zedelashvili, “Caucasus International University” Tbilisi, 2017.