Journal in Humanities; ISSN: 2298-0245; e-ISSN: 2346-8289; Volume 10, Issue 2, 2021

U.S. Cybersecurity Strategy as One of the Main Directions of National Security Policy of the Country

Nika CHITADZE[1*]

Abstract

The paper discusses the history of cyber warfare, its essence, basics and origins, the Internet, and technological advances. As well as threats from cyberwar, cyber-attacks, cyber defenses of different countries, viruses, malware and hacker attacks, information warfare, propaganda, disinformation, fake news, security concepts, and challenges. The main topic of the research is cyberwar, as a process following the real conventional war, as well as an alternative version of the war. There are analyzed global security, the role of the United States, and NATO. Based on the research, the paper separates and explains different terms, focusing on the political term "civil cyberwar" presented by discourse analysis based on new circumstances.

Keywords: Cybersecurity, Cyberwarfare, NATO, Security, Strategy, USA

[1] [*] Prof. Dr., Faculty of Social Sciences, Huminites and Education, International Black Sea University. Director of the Center for International Studies, Tbilisi, Georgia. Email: nchitadze@ibsu.edu.ge

Introduction

The social and economic well-being, health, and life of each citizen are highly dependent on the security of information systems and electronic services. Cyber-attacks have a great impact on all sectors of the economy, hinder the proper functioning of the economic space, reduce public confidence in e-services and threaten the development of the economy through the use of information and communication technologies. Against the background of the global cyber threats, when cyber attacks, cyber espionage, cyber terrorism, and disinformation are carried out on a daily basis, the development, introduction, and development of new defense mechanisms is an important issue. It is noteworthy that the US and NATO play an important role in this direction and together with the EU are a kind of security umbrella for both member and partner countries.

Each century is accompanied by its own problems. Cybercrime has become one of the most dangerous events in the 21st century - with many people, private companies, and government agencies being harmed on a daily basis. Billions of dollars are already being spent on defense.

All the concepts and doctrines of the US and NATO emphasize that according to the basic principles, no member state should be forced to rely only on its own strength. The Alliance Strategy allows each Member State to pursue national security objectives through collective means.

With the exception of the United States, every leading country in the world has a national cyber security strategy, which is a defining factor of state policy. The National Security Strategy aims to identify, prevent, reduce and eliminate existing threats.

Threats cannot be avoided without modern technology, professional staff, and cooperation with leading states. Consequently, the only way is international cooperation.

The US and NATO are the main forces that have the technical, financial, or human resources to withstand cyber threats. Therefore, it is important to study, analyze, research the current situation and future plans from a practical point of view. Researchers argue that if the scientific approach is correct, cyberbullying results will not be as devastating as they were in previous years.

Research Goals and Objectives

Depending on the subject matter of the study and in order to better identify new types of threats, which are reflected in the impact that cyber warfare has on world politics, as well as the analysis of new political conflict, specific goals and objectives of the study can be identified.

The Main Objectives of the Research are:

Identify cyber warfare as a new threat factor and discuss it in the context of a specific political conflict

Study and analysis of US security issues within the cyber security format

Identify the authorial definition of civil cyber warfare and explain its impact on political processes

The Main Research Questions of the Paper:

1. To what extent can cyber warfare be perceived as a new reality of political conflict?

2. What impact can cyber warfare have on the international community?

3. What is the US-NATO Action Plan and components of the military strategy in the context of cyber warfare?

Subject and Object of Research

The subject of research - Risks and threats to national security in the context of cyber and cyber threats in the process of a new dimension of political conflict in modern world politics.

The object of study - the role of the US and Euro-Atlantic Alliance in cyber defense and international security.

Research Methodology

1. Behaviorism Theory - A school of psychology founded in 1913 by John Watson (1878-1958). The school names behavior as a subject of study in psychology, with the aim of predicting and controlling behavior. Responding to Watson’s research, I. Pavlov’s work further strengthened behaviorism as a scientific approach. There are several forms of this theory: methodological behaviorism, radical behaviorism, experimental behaviorism. The theory is applied in terms of the cyber-behavioral approach, which is also actively used by the US military.

2. Theory of Political Realism - Science claims that political realism was the answer to liberalism, which was based on the premise that states do not seek cooperation. Early realists Edward Carr and Hans Morgenthau believed that states were selfish rational actors seeking power because of their own security concerns. Any kind of cooperation between countries is perceived as random. For the realists, World War II was a kind of confirmation of their ideas. According to the theory of political realism, international relations are fierce competition between countries that have no reason to trust each other when the essence of their existence is self-preservation in an environment where the loss of one is the gain of the other.

3. Balance of forces, or balance of forces - this is one of the oldest concepts in the theory of international relations. It is closely linked to political realism and stems from the anarchic structure of the international system. According to this theory, because the international system is anarchic, the main task of each state is to fight for self-preservation and self-determination. The necessary condition for this is security and independence. To maintain their independence and security, states act together to confront a state (or group of states) that threatens their security and sovereignty. Thus, the international system is divided into several groups of states that are approximately equal in strength, and the balance of power between them is the main guarantor of peace and order in the international system, the main condition for the stability of this system.

We have used this theory against the background of the development of cyber technologies to determine the existing balance of geopolitical forces and to assess the balance of forces, i.e. the balance of forces in cyberspace. The development of technology and cyberspace has to some extent changed the way countries make decisions, create policies, and interact with each other, so it is important to analyze the geopolitical situation according to this theory.

4. According to Richard Cohen's theory of "collective security", the following concept is presented - individual security, collective security, collective defense, and maintaining stability. Richard Cohen's theory can be said to be the cornerstone of NATO security, as defined in Article 5 of the Charter of this organization. It also applies in terms of cyber threats. We have used this concept of collective defense in this regard, an important guarantee of which is the joint work of NATO and the EU with both member and non-member countries.

Research Methods Used During Topic Development

Review, analyze and draw conclusions from existing theoretical material, which is also based on the basics of empirical research.

Qualitative research methods:

Narrative and descriptive - provides sources of narrative. For example history, diaries, biographies, memoirs, and descriptions.

Content analysis - Content-analysis method, which is related to the study of information disseminated by the media.

Event-analysis method - the study of political reality. The method is used to analyze the dynamics of politicians' interactions. The paper is used to analyze the dynamics of relations between politicians of different countries, including Georgian politicians.

Policy research analysis - globally, regionally, and locally. This issue is presented in the paper both from a geopolitical point of view and in relation to the cyberpolitical space.

The Concept of the Cyber Domain and the 21st-Century International Security System

We see physical tools such as computers, cables, cell phones, and so on. Tools interact in the virtual and unreal spheres. This facilitates the production of war from one part of the earth to the other, and the identification of the culprit is not always possible. Cyberomass is often the conceptual framework behind traditional warfare - including demonstrations of force, physical harm, and violence. As time goes on, it becomes more and more important to specify what type of cyber attack should be called cyber warfare. These types of definitions are important in resolving cyber-related issues, sometimes involving both kinetic and sometimes non-kinetic attacks. We have already discussed the difference between a cyberattack and a cyber-attack - there have been many attempts around the world to pinpoint the essence of cyber cyberbullying at a conceptual level, such as the Tallinn Handbook under NATO's Cyber Defense Cooperation Skills Center. However, it is not a political, official document of NATO. The difficulty, in this case, is that nation-states and non-state actors do not always obey the laws. We think that some topics in the "Tallinn Handbook" are incompatible with general, superficial, and theoretical definitions of cyberspace and need to be refined. For example, in the Tallinn Handbook, cyber warfare is equated with a cyber-attack - it is said to be an offensive or defensive operation that can result in death, injury, or destruction of objects (Ranger, 2018).

In our opinion, this definition excludes psychological pressure during cyber operations or cyber intelligence. The main drawback of this definition is the discussion of cyber and cyber attacks as one term. Also, this definition excludes cyber operations, which may be aimed at destabilizing the financial system of states. In this case, the cyber attack will not result in death or physical destruction.

The Importance of Cyber Security in the 21st Century

The terms "cyberspace", "cyber security", "cyberwar" have gained special relevance in the 21st century. Given this is an issue with which problems have no boundaries. As for the definition of the term "cyberspace", its exact definition is still under discussion. At the same time, all definitions state that it is an interconnected complex of information-technology infrastructure, which includes the global Internet, computer systems, telecommunication networks, and processors. "Cybersecurity" refers to technologies, processes, and practices designed to protect a network, device, data, or software from being attacked, damaged, or unauthorized accessed. Cyber security is also called information technology security. In turn, "cyber army" - unites cyber groups, cyber units. It can include all citizens who can work with computers, use IT technologies and take care of the state cyber security.

The creators of the Internet probably could never have imagined that with the increasing development of Internet technologies, a system of large-scale systems would be created whose security would be transformed into a significant challenge. Scientific-technological progress in turn, along with many positive elements, has created new threats and a new field of combat space. Cybercrime is committed against individuals, businesses, or governments on a daily basis. Today, cyber-attacks are a threat posed by leading national security experts.

One of the main problems in the fight against cybercrime is the fact that it is often very difficult to pinpoint not only the direct perpetrators but also their location or the country from which the attack took place. Therefore, an offender or a group of criminals can easily hide not only their involvement in organizing a cyberattack, but also identify themselves as other users of the network or remain anonymous altogether. The sources of cyber threats are representatives of the public and private sectors, as well as organizations and individuals created of different types and brands.

Sources of origin of cyber threats can be:

The state, with the help of its intelligence services, carries out cyber-attacks against potential adversaries in order to misinform, destabilize, intimidate or produce large-scale cybercrime. In addition, the special services of the state may resort to actions that are used to copy, steal and use citizens' personal data.

Corporations - engaged in industrial corporate espionage or subversive activities. In all of this, they often use hackers and organized crime groups. They can also violate human rights by collecting and analyzing personal data.

Hackers - the actions of most of them are criminal in nature. For a cyber attack on a selected site, it is enough to download the relevant instructions and protocols from the Internet and use them. Because of this, cyber-attacks have become easier for users to execute, in turn, hacking services are used by companies, corporations, intelligence, or other services.

Hacktivists - The term refers to the phenomenon of social protest. To achieve political goals, hacktivists can damage or disable some websites altogether.

Cyber saboteurs- are dissatisfied users and pose a serious threat. They are well acquainted with the principle of operation of the system and can use this knowledge for destructive purposes. For example to damage the system or to obtain confidential information.

Terrorists - they try to dismantle or destroy important objects altogether. Their actions endanger the national security of the countries. It causes massive human casualties, weakens the economy, harms society, and reduces their credibility with the government.

A botnet is the most common practice today. An Internet bot is a program secretly installed on a victim's computer. This type of hacker infects a large number of computers with its programs.

Fishers - These are individuals or small groups that use phishing technologies to steal personal details and sell valuable information. They often use "spam" and spyware.

Spammers - individuals or entities that massively send unsolicited e-mails with hidden or misleading information aimed at carrying out cyber-attacks on specific organizations using phishing and spyware.

The main features of cybercrime are the development of mass-negative social networks, the creation of malicious websites, the continuous mode of viruses and mass fraud, cyberterrorism, cybercrime, cyber warfare. The term cyberspace was first used in an extensive article in 1982.

Cyberspace is associated with everything related to the Internet. Cyberpunk - a subgenre of science fiction, the term first appeared in the New Wave science fiction novels in the late 1960s and early 1970s. As for the definition of cybersecurity - its first use was in the scientific literature in 1989.

Cybercrime - There are many forms of crime: financial, fraud, cyberbullying, theft, and any crime on the internet. Cyberdefense - This word is the same as cyber security, it is the detection, prevention, and response of cybercrime. This is more often the case with military and government systems. Cyber operations include cyberspace and are carried out both technically and non-technically. Cyberdelic - is related to the art, healing, or impressive experience that is accomplished through the active use of the Internet. Cyborg - Technically refers to the synthesis of cybernetics and the body, it means that it consists of robotic parts. Cybrarian - A cyber librarian, is a researcher who uses the Internet primarily for information. Cybernauts - A cybernaut is a person who creates sensory and virtual reality devices. Cybercrime, cybercrime, cyberterrorism, cyberattacks, and similar events are commonplace in modern life.

The Concept of Cyber Warfare and NATO

When we talk about the cyber concept and the issue of security, we must consider it in the context of the North Atlantic Alliance - security and cyber defense are directly related to NATO. The need to strengthen defense against cyber-attacks was first discussed by NATO member states at a summit in Prague in 2002. Cyber security has since become an important component of NATO’s agenda. The first cyber defense policy document was adopted in 2008. The process of integrating cyber security into the NATO defense system has been active since 2012. At the Wales Summit in 2014, the Allies made cyber defense a key part of their collective defense, 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 one of their key defense areas and agreed that NATO should protect itself in cyberspace as effectively as on land, sea, and air. NATO’s main partner in the field of cyber security 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 related to 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 defense. In 2016, the UK announced that it had allocated 9 1.9 billion to strengthen its cyber security program (Reuters, 2014).

At the 2018 Brussels Summit, the Allies agreed to establish a new cyberspace operations center. Given the common challenges, NATO and the EU are strengthening cooperation in the field of cyber defense, especially in the exchange of information. Joint training and research are conducted (NATO, 2018).

The Role of the U.S. in Cybersecurity Policy

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 U.S. 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). Defense spending around the world 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). As far back as 2007, the United States Air Force established Cyber Command, which lasted until the end of 2008, when these functions were transferred to the Air Force Space Command (European Law, 2018).

In May 2011, the United States unveiled its cybersecurity strategy, which is based on a model of cooperation with international partners and the private sector. The activities should be carried out in seven directions:

1. Economy - attracting international standards and innovations, open and liberal markets;

2. Protection of the national network - increasing security, reliability, and sustainability;

3. Legal side - expansion of cooperation and legal norms;

4. Military field - readiness for modern security challenges;

5. Government Internet Network - Expanding the efficiency and diversity of government structures;

6. International Development - Organizing security, developing international competencies and economic prosperity;

7. Freedom on the Internet - Support for Citizens' Privacy and Freedom (THE WHITE HOUSE, 2011).

How many kinds of concepts can there be in the world today? In addition to the important concepts that the United States, the European Union, NATO, all countries have their own national action plan, the most noteworthy is the new strategic concept approved at the Lisbon Summit in 2010 (NATO, 2011), according to which the United States established cyber-command. It was a response to Russia's actions. Whether or not Vladimir Putin came to power, he approved a new doctrine of information security (Cybersecurity Documents, 2000), the strategy of which was to give the government the right to control information and media networks. Putin also signed a legislative change - giving the tax police, the Interior Ministry, the Kremlin parliamentary and presidential security services, the border guard, and the customs service the same rights that only the Federal Security Service had.

On December 18, 2017, the first "National Security Strategy" (US National Security Strategy) (2017) was published by US President Donald Trump, which formed the basis of strategic documents such as the "National Defense Strategy" of the US Department of Defense. The strategy is based on four important national interests:

1. Protecting the American people and the American way of life;

2. The rise of American prosperity;

3. Maintaining peace;

4. Increasing American influence.

Interesting is chapter 3 of US Security Strategy, entitled "Maintaining Peace by Force", which claims two states - Russia and China:

"Russia is perceived as an existential threat to the United States. Russia is trying to restore the status of a great state and create its own spheres of influence near the borders. Its goal is to weaken US influence, eliminate allies and partners. The threat posed by China is seen as an increase in nuclear arsenals and military strength, as well as a desire to expel the United States from the Indian and Pacific regions, an attempt to bring order to the region and to establish desirable economic rules" (US Embassy Georgia, 2017).

The handbook, Cyber Dragon - China Information Warfare and Cyber Operations, authored by researcher Dean Cheng, notes that over the centuries, Chinese leaders have analyzed the most important technological advances that have helped China improve its global position. They realized the importance of information control as one of the powerful elements in maintaining power. Cheng also focuses on the development of war species:

"The development of technology has affected the economy and society, as well as the nature of war. Historically, war has developed, with mankind developing swords, spears, and other "cold weapons," or replacing them with rifles, grenades, machine guns, and so on. Today, humanity has moved from "hot weapons" to "soft power" at the expense of technological advancement" (Cheng Dean, 2017).

That is why the title of Chapter 4 of the new US strategy explicitly states:

"Increasing American Influence," which focuses on America's role, influence, and active participation in international institutions. In the event that existing institutions and regulations need to be modernized, the United States will lead the process," the document states (US Embassy, Georgia, 2017).

When it comes to increasing US influence in Donald Trump's strategy, it is obvious how the White House handles international relations, but it is difficult to say how real it will be when it comes to Russia, for which politics and ethics, fulfillment of promises and justice are far away.

Conclusion

Cyber security is a relatively new field in the modern world. Globally, there is a problem of lack of legal framework and international standards in the world, which, given the globalization and the modern world order, complicates the process of developing a regional and national cyber security strategy. Nevertheless, cybersecurity mechanisms largely depend on the experience of a particular country. As for NATO and the United States, as well as individual EU countries that have and spend large sums of money in this area, a number of facts prove that neither of these zones is fully protected.

References

Dean, Ch. (2017). *Cyber dragon, inside China s information warfare and cyber operations, The Changing Face of War.* James Jay Carafano, Series Editor, Publishing House "Praeger", USA, 2017 Y. P. 79-82.

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.Retrieved from: https://www.cnet.com/news/obama-adds-14b-to-budget-for-stepped-up-cybersecurity/

Homeland Security (2020). Department of Homeland Security Statement on the President's Fiscal Year 2021 Budget. Retrieved from: https://www.dhs.gov/news/2020/02/11/department-homeland-security-statement-president-s-fiscal-year-2021-budget

MFA of Russian Federation, (2000). INFORMATION SECURITY DOCTRINE OF THE RUSSIAN FEDERATION. Retrieved from: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Russia_2000.pdf

NATO, (2011). Edited by Jens Ringsmose and Sten Rynning, NATO's NEW STRATEGIC CONCEPT: A COMPREHENSIVE ASSESSMENT. Copenhagen, DIIS. DANISH INSTITUTE FOR INTERNATIONAL STUDIES, 2011 Y. Retrieved from: https://www.econstor.eu/bitstream/10419/59845/1/656748095.pdf

NATO, (2018). Brussels Summit Declaration - Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Brussels 11-12 July 2018. Retrieved from: https://www.nato.int/cps/en/natohq/official_texts_156624.htm.

Ranger, S. (2018). What is cyberwar? Everything you need to know about the frightening future of digital conflict. Retrieved from: https://www.zdnet.com/article/cyberwar-a-guide-to-the-frightening-future-of-online-conflict/

Reuters, (2014). France to invest 1 billion euros to update cyber defenses. Retrieved from: https://www.reuters.com/article/france-cyberdefence-idUSL5N0LC21G20140207.

RIAC, (2016). NATO's Cyber Defense Evolution - NATO's New Digital Wall. Retrieved from: https://www.nato.int/docu/rdr-gde-prg/rdr-gde-prg-eng.pdf.

The White House, (2011). INTERNATIONAL STRATEGY FOR CYBERSPACE, Prosperity, Security, and Openness in a Networked World, Washington, 2011. Retrieved from: https://www.hsdl.org/?view&did=5665.

The White House, (2017). The United States of America, National Security Strategy, Washington. Retrieved from: https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf

US Embassy in Georgia, (2017). US National Security Strategy. Retrieved from: https://ge.usembassy.gov/ka/2017-national-security-strategy-united-states-america-president-ka/