https://doi.org/10.35945/gb.2024.17.008

INFORMATION WAR – INTERNATIONAL SECURITY DILEMMA IN THE MODERN WORLD

TAMTA CHEISHVILI tamta.cheishvili@atsu.edu.ge

Assistant Professor, Akaki Tsereteli State University, Georgia

TINATIN KOSTAVA Tinatin.kostava@atsu.edu.ge

Assistant Professor, Akaki Tsereteli State University, Georgia

Abstract. In the modern world, in the field of international security, one of the important challenges is the information war. On the other hand, information is a universal and cheap weapon with a limitless scope and high efficiency. Therefore, it can be more dangerous than any conventional means of warfare. During its implementation, the attacking side achieves the desired outcome through the psychological manipulation of common beliefs. During the last ten years, the rate of disinformation has increased sharply. Also, propaganda, espionage, uncontrolled dissemination of state secrets and personal information, massive cyber-attacks and so on. Both states and terrorist organizations use such mechanisms. Today, the most functional means of information in this field are used by terrorist organizations, which often use social media to recruit so-called "Islamic Fighters" and lay out fundamentalism. Cooperation at the international and regional levels is important in fighting cybercrime and protecting critical information infrastructure. For this purpose, within the framework of the Council of Europe, the European Union, the United Nations, NATO, and other international organizations, it carries out active activities on cyber security topics. In addition, protecting against cyber intrusion, even on a small scale, is in the country's national security interests, and it is crucial to involve each state in the proceeding discussion about information warfare.

KEYWORDS: INFORMATION WAR, INTERNATIONAL SECURITY, "ISLAMIC STATE"

INTRODUCTION

In the modern world, in the field of international security, one of the important challenges is the information war. In its broadest sense, information war is a fight through information to gain a specific advantage. Over the past few decades, the rapid growth of information and communication technologies and their increasing distribution have significantly increased the importance and consequences of information warfare. In the 21st century, in the conditions of broken boundaries between war and peace, the escalation of conflict, according to the causes and features of detection, is significantly related to information. Information conflicts, in terms of a general theoretical approach, are recognized by specialists in the field as one of the five main types of conflict, the origin of which is related to the scarcity-abundance of information, disinformation, and propaganda, and

it can be equally dangerous in a closed totalitarian as well as in a democratic society.

This is unequivocally confirmed by the current political processes in the world (Jorbenadze, 2001, 31) [1].

MAIN PART

Information warfare is a modern concept that uses information technology to gain an advantage over an adversary. Current events in the world have made it clear how vulnerable this or that society can be in the case of information manipulation and how public opinion changes under the conditions of information management.

Because information is a universal and cheap weapon, with an unlimited area of action and high efficiency, it can be a greater threat than any traditional means of war. At first glance, it does not bring devastating results from a physical point of view, such as is inevitable in the case of an armed conflict. Still, the success of information warfare is mainly expressed in the fact that, during its implementation, the attacking party can crack the opponent's institutional structure and universally recognized fundamental values, confuse them and limit the truth. And lie between reality and illusion to achieve the desired result by psychologically manipulating public opinion. However, there are more active methods in the information warfare framework; the initiating party has various means to fulfil the set goal. These are:

1. 1) Cyber-war (cyber-attack) – "the action of a state-nation aimed at penetrating the computer network of another state, to cause damage to the latter or to completely disable it". In other words, it is a complex of offensive measures carried out in cyberspace or by several states and directed against another state or international non-state entity;
2. 2) Cyber-terrorism, which is used by terrorist organizations in cyberspace and is directed against the national security of the country;
3. 3) Anti-cyber-terrorism, used against terrorist organizations and carried out in cyberspace;
4. 4) Cybercrime is used by various criminals or transnational groups, during which cyberspace is used for theft, information theft, fraud, etc. Sh. Their objects can be both individuals and large companies. Its purpose is to obtain economic profit;
5. 5) Anti-cyber crime includes protective measures by state law enforcement or private individuals and companies against cyber criminals (Svanadze, 2015: 20-21) [2].

The information war consists of two main stages: a) the information-psychological period, which takes place in the conditions of information competition, continuously and affects the armed forces of the opponent, the population, and political and intellectual elites; b) the information-technological period, which is activated directly during hostilities. In this case, information is collected, processed and transmitted to achieve specific tasks, including illegal methods. Of course, one-time actions cannot achieve the result, and the system must operate continuously for years with sensitive topics identified by the special services, which are precisely selected for the target groups (Khidasheli, 2017: 7) [3].

The following groups can be singled out as initiators of the information war:

- National subversive groups;
- National and transnational criminal groups (Mafia, Yakuza, Triad, Camorra);
- Terrorist organizations;
- Multinational companies with their financial means;
- Companies with foreign capital;
- Extra-parliamentary opposition groups (right-wing extremists, xenophobic groups);
- Religious sects;
- Hacker groups;
- Other state and national military-political, as well as financial associations;
- Associations, foundations, non-profit organizations;
- Non-governmental and international organizations;
- Political organizations and trade unions;
- State institutions (Svanadze, 2015: 21-22).

The unprecedented scale of the scientific and technical field development led to opportunities for introducing new technologies, which do not

always serve to create public good. Moreover, if they are used for an irrational, destructive purpose, the world's superpowers and international organizations become vulnerable. Understanding this threat forced the leading actors of modern international relations to name cyber and hybrid threats as the main challenge for the organization's member states at the 2016 NATO Warsaw Summit (Warsaw Summit Communiqué, 2016) [4].

Although modern technologies are the greatest achievement of the civilized world, we cannot ignore the problems related to technological progress. Over the last decade, the rate of disinformation spread through the Internet has increased significantly. Also, propaganda, espionage, uncontrolled dissemination of state secrets and personal information, massive cyber-attacks and so on. Such methods are used by both states and terrorist organizations, and in this way, Russia launched active attacks against Georgia during the 2008 war (Gotsiridze, 2019) [5]. However, when it comes to talking about Russia in the named context, special attention is drawn to the events that developed around the US presidential elections. The reports developed as a result of the investigation, together with the statements made by Donald Trump, completely overshadowed the list of cases that the Russian side conducted even against Ukraine or Georgia. In the presidential elections of the United States of America, he tried to help a specific presidential candidate win by means of internet manipulations, information propaganda and cyber attacks, which is confirmed in the reports of the US Central Intelligence Service (Entous, 2016) [6].

Today, the most active means of information used by terrorist organizations, which are the so-called Social media such as Facebook and YouTube, are often used to recruit "Islamic fighters" and spread fundamentalism. Terrorist organizations also create special pages blogs, where they spread extremist materials and ideas, engage in propaganda, and publish photo and video material depicting terrorist activities carried out by them, thus successfully sowing panic among the population and directly in those specific individuals, financial institutions or political organizations. against which the mentioned list of actions is directed. In 2015, a series of terrorist attacks in Paris was preceded by a series of no less large-scale cyber attacks, the targets of which were both state and private organizations. In addition, the companies whose activities were connected to France and French companies in various ways became the objects of active hacking attacks. Groups suspected of cyber terrorism: "the Middle Eastern Cyber Army" (the Middle Eastern Cyber Army – MECA), Fallaga Hackers Team and Cyber Caliphate. According to The National Interest, the Cyber Caliphate is linked to the so-called "Islamic State" (ISIS) (King, 2015) [7]. In the last decade, especially in Syria, since the intensification of hostilities and the emergence of the so-called "Islamic State" ISIS, the number of cyber attacks has practically doubled. For example, from the reality of our country, we can name the activation of the terrorist organization ISIS in the Georgian Inter-

net space in 2015 and the creation of a page by it, which served to implement all the goals named above. The website was saturated with various types of information, such as a propaganda photo gallery, official appeals to Georgian Muslim youth to join the fighting activities carried out by the Islamic State, letters from various members of the terrorist organization, and video materials depicting scenes of execution of opponents. It should be noted that the site only existed for a few months and later, Georgian special. It was blocked as a result of the services.

Cooperation at the international and regional level is of great importance in fighting cybercrime and protecting critical information infrastructure. Similar cooperation in cyberspace protection includes international and regional conventions, forums, organizations and alliances, meetings and discussions, joint resolutions, decisions and recommendations, and directives. Within the framework of the Council of Europe, the European Union, the United Nations, NATO, and other international organizations, it carries out active activities on the topic of cyber security. In addition, protecting against cyber intrusion, even on a small scale, is in the country's national security interests, and it is important to involve each state in the ongoing discussion about information warfare.[1]

CONCLUSION

In the end, we can conclude that the threats caused by the information war equally threaten the Internet space, both locally and internationally, which creates a great challenge in terms of international security. Cyberspace is less secure, and therefore, the number of cybercrimes is increasing irreversibly. In such a situation, great importance is attached to cooperation at the regional and international levels, the direct purpose of which is developing a common defence mechanism. In addition, efforts by the state to raise public awareness in this area are equally important, as they will reduce risks at the local and global levels.

1 Author's note: The site is currently blocked in response to threats from the Georgian government and the named materials are no longer searchable – https://xalifati.files.wordpress.com

REFERENCES:

1. Jorbenadze R. (2001). Management of Political Conflicts, Tbilisi, "Science".
2. Svanadze V. (2015). Cyberspace and Cyber Security Challenges (Collection), Tbilisi.
3. Khidasheli T. (2017). From World War II to Cyber War, How to Win the Information War? Tbilisi, Georgian Strategy and International Relations Research Foundation.
4. Warsaw Summit Communiqué, Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8-9 July 2016 – https://www.nato.int/cps/en/natohq/official_texts_133169.htm [Last Access: 30.05.2024]
5. Gotsiridze A. (2019). The Cyber Dimension of the 2008 Russia-Georgia War, 2019 – https://gfsis.org.ge/ge/blog/view/970 [Last Access: 30.05.2024].
6. Secret CIA assessment says Russia was trying to help Trump win White House, By Adam Entous, Ellen Nakashima and Greg Miller, December 9, 2016 – https://www.washingtonpost.com/world/national-security/obama-orders-review-of-russian-hacking-during-presidential-campaign/2016/12/09/31d6b300-be2a-11e6-94ac-3d324840106c_story.html [Last Access: 30.05.2024].
7. The National Interest, Why to Fear ISIS's Cyber Caliphate, 2015 – https://nationalinterest.org/blog/the-buzz/why-fear-isiss-cyber-caliphate-12023 [Last Access: 30.05.2024].