International cyber security challenges

Duić, Igor; Cvrtila, Vlatko; Ivanjko, Tomislav

International cyber security challenges

I. Duić*, V. Cvrtila**, T. Ivanjko***
*Croatian Radiotelevision, Zagreb, Croatia
** University of Applied Sciences Vern, Zagreb, Croatia
***Faculty of Humanities and Social Sciences/Information and Communication Sciences, Zagreb, Croatia
igor.duic@gmail.com

Summary - The opportunities provided by the information and communications technology, with a special emphasis on the Internet, have become an integral part of life. However, are we sufficiently aware and prepared as individuals, nations or the international community for the threats coming from cyberspace or for the denial of the use of that dimension of communication, commerce and even warfare? Namely, despite the growing number of users, the Internet is still beyond or below minimum regulation. Those are precisely the conditions for the organization and realization of hostile action in cyberspace. There are security issues within the cyberspace that represent a security risk and challenge of modern times.

The development and application of the information and communications technology has created a new battleground. As a special challenge to international security, cyber terrorism arises. Cyber security will significantly affect international relations in the 21st century. This paper gives an overview of the concepts and principles of cyber threats that affect the safety and security in an international context.

Keywords: cyberspace, cyber-attack, cyber terrorism and crime, international security.

I. INTRODUCTION

Cyber warfare and terrorism 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. Even though cyber threats have in the recent years been specifically emphasized in the modern military doctrines of great powers and NATO, they are still shrouded in secrecy.

The purpose of this paper is to draw attention to cyber threats, which endanger the safety of modern states, organizations and international relations. By combining the principles of a review and professional research paper, this paper aims to show cyberspace, in terms of security challenges, as a dimension in which international relations unfold. It is necessary to distinguish the main subjects of the international cyber security environment, analyze their intentions and set a paradigm of the multipolarity of cyberspace and analyze its uniqueness and principles.

NATO's Strategic Concept, adopted at the end of 2010 at the Lisbon summit, determines that cyber-attacks have become more frequent, more organized and more expensive, causing damage to the government administration, the business sector, economies, and potentially to the transport and supply. It also states that cyber-attacks can reach the level that threatens the national and Euro-Atlantic prosperity, security, and stability. Foreign military and intelligence services, organized criminals, terrorists and extremist groups are the potential sources of such attacks. What is also emphasized in the conclusions of the Lisbon summit is the need to further develop the skills of prevention, recognition, defense and recovery from cyber-attacks, including the use of the NATO planning process for the advancement and coordination of the national abilities of cyber protection, assembling all NATO bodies under a centralized cyber protection, and a better integration of the NATO cyber awareness, warnings and common response of the member states [1].

It should be borne in mind that the rapid development and adoption of technologies through their use in everyday life opens up many opportunities for the attackers, whether they are in the form of states, terrorists or criminals, because they are always at an advantage in cyberspace. We can therefore conclude that, a new concept of cyber security in which prevention represents a significant portion is being created.

The initial hypothesis is that cyberspace is a growing security risk and challenge of modern times. Moreover, cyber security will significantly affect international relations in the 21st century, while the threats and challenges will exponentially increase.

The goal of this paper is the synthesis and analysis of knowledge based on a review of recent literature and professional and scientific articles that problematize the challenges of international security in cyberspace. The scientific work seeks to show cyberspace as an operational dimension of international relations in terms of the cyber security challenges. With the systematization of the cyber warfare strategy and the very methods of attack, links with

the planned action will be set up through the application of technical, computing and network systems.

II. INTERNATIONAL CYBER SECURITY

The cyber domain has a great influence on the transformation of the international security and the very concept of security. Many authors highlight the necessity of the duly understanding and setting up of cyber doctrines.

The new, cyber dimension of international relations is a major challenge for the theories of the preservation of power and intimidation. Cyber threats are serious, destabilizing and on the increase. The theories and strategies of intimidation designed and implemented during the Cold War cannot be implemented in the cyber domain. Many scientists are working on the understanding of the cyber revolution in international relations. Authorities have also taken certain steps in cooperation, especially in the area of crime and the establishment of CERTs (Computer Emergency Response Teams) [2]. Tatalović, Grizold and Cvrtila write that the processes of internationalization and globalization have brought a greater cohesion and efforts for a unified regulation of the world order, more than it was in the system of sovereign states during the Cold War. This is reflected in the core of the states' security policies. In that context, a new concept – human security concept – emerged in theory and political practice. In contrast to the traditional concept of national security, it primarily emphasizes the security of an individual, not the state [3]. Lin theorizes [4] about cyber security. The concept of intimidation was the basic idea of the nuclear strategy. However, the question is whether the dissemination of the principles of intimidation on cyberspace is a viable strategy. Even though nuclear and cyber weapons share a key feature – the superiority of the attack in comparison with the defense – they differ in many ways. Only a few countries possess nuclear weapons and the number of possible enemies is limited, as is then the application of intimidation. The situation is completely different when it comes to cyberspace. Unlike nuclear weapons, each state has access to cyber "weapons", and such attacks cannot be firmly linked to state action. The protection of national infrastructure against attack could become another common interest of states. Experts and analysts estimate that the efforts of Russia and China to dominate cyberspace have over the past few years intensified so much that any delay in this area could present a big problem for the modern West.

Cyber-attack, whether it happens as a conflict between states, a terrorist or a criminal act, is an attack in cyberspace with the aim of compromising a computer system or network, but also of compromising physical systems as it was the case with the Stuxnet worm. In layman's, popular terms, most often mentioned in the media, it is called a hacker attack. Identical methods of a hacker attack are applied for both military and terrorist purposes.

Janczewski and Colarik [5] divided cyber-attacks into phases, which they consider to be basically the same as the phases of conventional criminal offenses:

- the first phase of the attack is the scouting of potential victims. By observing the implementation of the normal operations of targets, useful information that are accumulated and determined through the used applications and hardware;
- the second phase of the attack is intrusion. Until the attacker gets into the system, there is not much that can be done against the target apart from disrupting the availability or access to certain services provided by the target;
- the next phase is the identification and dissemination of internal opportunities by examining the resources and the right to access the restricted and important parts of the system;
- in the fourth phase the intruder does damage to the system or steals certain data;

Furthermore, they indicate that today cyber-attacks consist primarily of:

- malware via attachments in the Internet browser, e-mail or other system vulnerabilities;
- denial of service (DoS) to prevent the use of computer systems and networks;
- deletion or transformation (leaving a message) to government and commercial websites for propaganda purposes or in order to disrupt the informing;
- unauthorized intrusion into systems for the theft of confidential and/or proprietary information, compromising of data or using the system in order to launch attacks against other systems.

In such circumstances of transformation and different views and understandings of security in general and international security, cyber threats certainly redefine those terms. In line with the efforts to ensure security on one hand and specificities of cyber threats and motives of the actors who initiate them on the other, it will be necessary to set up a new international security paradigm of the cyber age.

III. MULTIPOLARITY OF CYBERSPACE

The USA, Russia and China are nations known for their skilled military cyber units. In addition to the aforementioned states, France and Israel are working on the development of cyber capabilities. American intelligence officers believe that there are 20 to 30 armies with respectful capabilities for cyber-war, including Taiwan, Iran, Australia, South Korea, India, Pakistan and several NATO countries. The United States Cyber Command, along with the agencies they work with, has some of the most intelligent, patriotic-minded civil servants, both military and civilian, who create plans and capabilities for the domination in cyberspace with the goal of preserving the national security and peace [9].

Strategic domination in cyberspace has not yet been achieved by any of the entities of international relations. That is undoubtedly the goal of many nations such as the

USA, China and Russia. However, as much as they might invest in their defense system and offensive capabilities, the system of power has not been set up. As opposed to the bloc division of the world into two centers of power during the Cold War, intimidation based on offensive capabilities is not crucial in cyberspace and there are many centers of power. The strength of those nations will mostly depend on the possibility of establishing an adequate defense system which is also influenced by their dependence on the information infrastructure. The dependence on information infrastructure is in correlation with the level of vulnerability of the economically and militarily developed digitized countries.

Due to the specificity of cyberspace, especially the asymmetry with the actual time and space and the geostrategic factors, a new security challenge that requires new military concepts is put before states and organizations. Namely, it is necessary to develop specific defense doctrines, but also offensive plans for action in cyberspace.

The dependence on networked computers and computer communication leaves the USA vulnerable to possible attacks, which made the cyber world a major source of uncertainty [6]. The vulnerability to attacks and the possibility of action is defined by Clarke and Knake [8] as the national cyber power. They state that the national cyber power is the net estimate of the ability of a nation to wage a cyber-war. National cyber power takes into account three factors: offensive cyber capabilities, national dependency on cyber networks and the nation's ability to control and defend its own cyberspace by implementing measures such as stopping the traffic outside the state. Based on these three factors, the authors provide an assessment of the overall cyber power of the United States, Russia, China, Iran and North Korea. To facilitate the comparison and analysis, the results of the assessment are systematized in the following table. The measurement scale goes from 1 to 10, with the smaller value representing a worse assessment and the higher value representing a better assessment.

Nation	USA	Russia	China	Iran	North Korea
Offensive capabilities	8	7	5	4	2
Dependency on the cyber network	2	5	4	5	9
Defensive capabilities	1	4	6	3	7

Table 1. Assessment of the national cyber power

They further explain why the USA, according to the assessment, is not the dominant power of cyberspace. If the total national cyber power was observed only on the basis of the offensive capabilities, the USA would occupy the first place. However, the outcome of a cyber-war does not depend only on the offensive capabilities. The important part is the dependence of a nation on the systems in cyberspace. Unlike the USA, China is developing its offensive cyber capabilities, but it is also oriented on the defense. Cyber warriors of the Chinese military have both offensive and defensive tasks in cyberspace and in contrast to the military of the USA, when talking about the defense, they also refer to the defense of the nation, i.e. the civil networks, not just the military networks. In China, the networks that make up their Internet infrastructure are under the control of the government. The Chinese government has the power and means to shut down the Chinese portion of the Internet from the rest of the world, which it would very likely do in case of a conflict with the USA. On the other hand, the USA has no plans or the capacity to do so, because their cyber connections are largely privately owned. China may limit the use of cyberspace in a crisis, refusing access to certain users. The USA cannot do it. North Korea has high scores when it comes to the defense and low dependence on the network infrastructure. Namely, that country may terminate its limited connections with cyberspace in an easier and more effective way than China. North Korea has few systems that are dependent on cyberspace that a large cyber-attack on its systems would have a minimal effect. The authors warn that one should bear in mind that cyber dependency is not the percentage of households with a broadband connection or the number of people who have smartphones, but the degree to which the critical infrastructure (electricity, railways, supply chains) dependent on the network systems. Thus, a state which is largely dependent on the systems in cyberspace has greater challenges in the creation of a national cyber defense. This is why the USA is more vulnerable to cyber-war than Russia or China. It is certainly more risky for the USA to engage in cyber-war than it is for a small country such as the North Korea. With three large entities of international relations (the USA, China and Russia) and the balance of power in cyberspace, the overall cyber power of two states that pose a threat to the world because of their totalitarianism and nuclear problems has been analyzed. Clarke and Knake estimate that they do not have great offensive capabilities, but have participated in the abuse of cyberspace.

The Iranian presidential election of 2009 sparked a huge public protest against election fraud. Social media platforms, mostly the two most popular, Twitter and Facebook, served for the organization, rebellion and spreading of anti-regime news. The Iranian government responded by introducing harsh police actions against the demonstrators, by shutting down media channels, and disabling Internet access within the country. Some members of the

opposition launched DDoS attacks (distributed denial of service) against the websites of the Iranian government. Due to the speed and ease of communication, they used Twitter to organize and recruit cyber activists. They also used it to exchange links on an software that facilitated the inclusion of participants in the DDoS attack [7]. It is clear from the available data that this is not an international, but intrastate conflict. This is by no means a cybercrime because the attackers were politically motivated.

Because of its nuclear program, Iran was a target of an attack by the computer worm Stuxnet in June 2010. The worm was created to infect the industrial systems, and it proved its danger by sabotaging the Iran's nuclear program. In addition to the Iran's nuclear program, it also infected thousands of computers and industrial facilities worldwide. The Stuxnet worm can hide in cyberspace for a longer period. Analysts disclosed that the complex worm was written specifically for the breaching and taking control of the computer systems of Natanz nuclear facility in Iran. The worm takes very good care of itself for a longer period in cyberspace. Experts describe Stuxnet as a sophisticated piece of software with half a million program lines of code. For such a complex malware, it is necessary to have knowledge of the certain types of industrial control systems that are being attacked, and it seems that the code was written by an expert team, and not just one person [11]. Therefore, there was a suspicion that it was done by American or Israeli programmers. In an article published in the New York Times, Sanger [12] writes that the American President Obama ordered the cyber-attack on Iran, i.e. on the centrifuges used for the uranium enrichment.

North Korea, due to its poor technological development, is not very dependent on the systems in cyberspace. That is also the reason behind the very good assessment of their defense capabilities. Even though it has no developed offensive capabilities, it is obvious that it has recognized the importance of playing an active role in cyberspace. In fact, in July 2009, a few dozen American websites, including the website of the White House, were under a DDoS attack (denial of service). The main suspect was North Korea. That status was confirmed after the attacks spread to South Korea. The South Korean media and government officials publicly accused its northern neighbor, and the officials of the USA advocated a cyber-counterattack “in order to send a strong message" [7]. In November 2014. a group which calls itself GOP or The Guardians Of Peace, hacked its way into Sony Pictures and stole the data that included personal information about the Sony Pictures employees and their families, e-mails between the employees, information about the executive salaries at the company, copies of the then-unreleased Sony films, and other information [9]. The purpose of the attack, attributed to North Korea, was to deter Sony Pictures from releasing a movie which was (correctly) understood as ridiculing that country’s dictator and portraying the North Korean regime and its leader, Kim Jong-Un, with sarcasm and mockery [10].

IV. CONCLUSION

The topic of the paper, cyber threats to international security, stands out merely by its title as an interesting and challenging area of research. The explanation for it is first and foremost that the area has not yet been sufficiently explored, especially not in the Croatian context. Due to the intensive development of international relations in cyberspace, conditioned and supported by the speed of the development of technologies and their implementation in the relations of states, organizations and individuals, this area will always be interesting and challenging. That conclusion arises from the constant change of attitudes and technology. It is precisely that instability which indicates that from that specific, interdisciplinary field of research, in 5 or 10 years, it will be possible to draw some new conclusions, and according to them, set some new paradigms and doctrines. Carr [7] states that cyber-warfare has been present for about a decade, but that it is still not well defined. There is no valid international agreement which would establish a legal definition of an act of cyber aggression. In fact, the entire area of international cyber law is still unclear.

The development and availability of information and communications technologies and the ever-present tensions between politically and ideologically different states have conditioned the international relations in cyberspace. Strategic domination in cyberspace has not yet been achieved by any of the entities of international relations. A large number of international entities demonstrated their presence and willingness to act in cyberspace. That demonstrates a multipolar dimension of cyberspace in which it is very unlikely that domination or bloc division will occur. The reasons lie in the mutual mistrust and fear of espionage in the case of linking the defense systems. However, the nations that are the most influential are the ones that are the most powerful, economically and militarily, and at the same time are the most dependent of the cyber-infrastructure – the USA, Russia and China. NATO also plays an active role. We can conclude that in the recent years, a new concept of cyber security that can be defined as a paradigm of the multipolarity of cyberspace is being created.

Most authors predict an escalation of conflicts and intelligence activities in cyberspace, which supports the confirmation of the initial hypothesis of this paper. They state that cyber-attacks are among the biggest threats to the international security. Unlike conventional conflicts, such attacks will become increasingly common, and they could, as a conventional attack, cause large-scale destruction, even with fatal consequences. It is therefore essential to establish an effective defense in which the key role is that of prevention, international cooperation

and the adoption of the internationally recognized, legally binding norms.

Due to the increase in cyber-terrorism and crime, it is necessary to organize systematic education and to strengthen operational military, intelligence, police and civil centers for the defense from cyber-attacks.

If we take into consideration all that has been stated in the elaboration, and the confirmation of the initial hypothesis, we can conclude that cyber security has become one of the prerequisites of the democratic concept of life in the modern society.

REFERENCES

[1] NATO, "Strategic concept for the defence and security of the members of North Atlantic Treaty Organization," 2010, Available: http://www.nato.int/nato_static/assets/pdf/pdf_publications/20120214_strategic-concept-2010-eng.pdf (3.2.2017.)

[2] N. Choucri and D. Goldsmith, "Lost in cyberspace: harnessing the Internet, international relations, and global security," Bulletin of the Atomic Scientists, vol. 68, no. 2, 2012, pp. 70-77.

[3] S. Tatalović, A. Grizold, and V. Cvrtila, Suvremene sigurnosne politike. Zagreb: Golden marketing-Tehnička knjiga, 2008.

[4] H. Lin, "A virtual necessity: some modest steps toward greater cybersecurity," Bulletin of the Atomic Scientists, vol. 68, no. 5, 2012, pp. 75-87.

[5] L. J. Janczewski and A. M. Colarik, Cyber warfare and cyber terrorism. Hershey: Information Science Reference, 2008.

[6] J. S. Nye, "Cyber war and peace," 2012, Available: http://www.project-syndicate.org/commentary/cyber-war-and-peace (3.2.2017.)

[7] J. Carr, Inside cyber warfare, 1st ed. Sebastopol, CA: O'Reilly Media, 2010.

[8] R. A. Clarke and R. K. Knake, Cyber war: the next threat to national security and what to do about it. New York: Ecco, 2010.

[9] Risk Based Security, "A Breakdown and Analysis of the Sony Hack," 2014, Available:
https://www.riskbasedsecurity.com/2014/12/a-breakdown-and-analysis-of-the-december-2014-sony-hack/#thebeginning (9.4.2017.)

[10] G. Siboni and D. Siman-Tov, "Cyberspace Extortion: North Korea versus the United States," INSS Insight No. 646, 2014, Available: http://www.inss.org.il/uploadImages/systemFiles/No.%20646%20-%20Gabi%20and%20Dudi%20for%20web.pdf (9.4.2017.)

[11] M. Petrović, "Obrana od cyber-napada", Hrvatski vojnik, vol. 9, no. 385, 2012, pp. 26-29.

[12] D. E. Sanger, "Obama order sped up wave of cyberattacks against Iran," The New York Times, 2012, Available: www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=1 (3.2.2017.)