ISSN No:-2456-2165

Cybersecurity in the New Reality: Systematic Review in the Context of COVID-19

Andreja Mihailović
Law faculty University of Montenegro
Podgorica, Montenegro

Neli Rašović
Ministry of the Interior of Montenegro
Podgorica, Montenegro

Abstract:- The Covid-19 outbreak and the subsequent lockdown dramatically changed the behaviour of billions of people across the world who switched to the digital space. In a matter of weeks, the restricted movement of people shifted work, connecting and entertainment to online. With the rise of social distancing, we have been directed to our devises for almost any activity, which has consequently increased our vulnerability from all forms of cyberattacks. If we consider the fact that we are living in times of progressive informatization of society it is realistic to expect the new scenarios for disruption of individual, corporate, national and global security. Cyberspace does not recognize geographical and political boundaries, therefore cyberthreats do not recognize borders between countries. The fact is that cyberspace is accepted as a legitimate battlefield (the so-called fifth battle space together with: land, air, sea and outer space) in strategic documents of most countries of the world. This, of course, further complicates relations in the international arena, setting new challenges for experts in international war law and humanitarian law, and actualizes the issues of international legislative harmonization. It is not necessary to emphasize the necessity for cooperation between international institutions responsible for cybercrimes, as well as the exchange of information between States, their regulatory bodies and security services to counter cyberthreats.

Keywords:- *Cybersecurity, Digitalization, Covid-19, Coronavirus, Cybercriminals.*

I. INTRODUCTION

We live in a time of progressive informatization of society where the number of Internet-connected devices is increasing at a galloping pace. According to a study presented by the IHS Markit more than 20 billion devices are currently connected via Internet. It is predicted that by the end of 2020, it will be at least 30 billion, while by 2025, the number will exceed an incredible 75 billion (IHS Markit, 2017). The constant progress of information technologies and the expansion of cyberspace greatly encourages the economic and social progress of every country in the world. Information security is in the common interest of all mankind and it refers to global peace and development, as well as to the national security of all states. However, this advantage brings with it new security risks and challenges (Ministry of Public Administration of Montenegro, 2018). Cyberspace knows no geographical or political borders and neither do cyberthreats know borders between states. It is a space in which we all participate, and from which almost no one is protected. As Frank Wolf describes it illustratively: "There are two kinds of people in America today: those who have experienced a foreign cyberattack and know it, and those who have experienced a foreign cyberattack and don't know it" (Gehrke, 2014).

There is no going back in thematizing cybersecurity and it can no longer be treated in segregation from real world security. If we take into account the fact that the progressive informatization of society is ongoing, that the number of devices connected to the Internet is increasing, it is realistic to expect the emergence of new scenarios for violating individual, corporate, national and global security. The fundamental problem is that cyberculture is evolving faster than cybersecurity, which further implies that cyberspace integrally is at a certain risk. Private data, intellectual property, infrastructure, and even military and national security can be compromised by deliberate attacks, unexpected security vulnerabilities, and the immanent vulnerability of the Internet. For this reason, it is important that Governments become aware of the need to partner with the private sector, citizens and other governments to reach an integrated transnational solution.

Access to information is crucial today. New business and government activities are based on digital connectivity and the entire national infrastructure has come under the control of complex computer systems. It is realistic to anticipate that traditional elements of life, such as houses or cars, will soon be able to get their IP addresses, ie. be plotted on a digital map and participating in it is no longer a matter of choice. The digital world faces two basic problems: the security of data transmission and the realization of secure communication. These are problems that always arise and that need to be addressed in order to gain confidence in the digital environment. As there are criminal acts in the real world, so they occur in the virtual world. It's a relentless modern form of crime, and the difference is that in the virtual world, a real criminal lurks behind his computer, and it's hard to be detected. Precisely because of this, only a small percentage of cybercriminals are liable for the damage they have committed. Even after the execution of his sentence, no one can guarantee that such an individual will not repeat the same mistake. Cybercrime - the crime of the modern, digital age. In order to gain the trust of individuals in doing business via Internet in a cyberenvironment, it is necessary to establish a security policy through information systems. It is a ruthless

form of crime for which a very small number of cybercriminals are liable. Information systems need to provide security policies to gain individuals' trust in doing business online. The difference is that in the virtual world, a real criminal lurks behind his computer, and it's hard to detect. Precisely because of this, only a small percentage of cyber criminals are liable for the damage they have committed. Even after the execution of the sentence, no one can guarantee that such an individual will not repeat the same thing. In its "X-Force Threat Intelligence Index" report, IBM presented that "8.5 billion records breached in 2019, giving attackers access to more stolen credentials" (IBM, 2020). A lot of energy is focused on the benefits that the digital world can provide to the economy, governments and society itself. However, now is the time to shift the focus to what benefits security can bring to the digital world.

II. DISCUSSION

The fact is that cyberspace is recognized as a legitimate battlefield (the so-called fifth battlefield alongside: land, air, sea and space) in the strategic documents of most countries worldwide. For several years now, some countries have been developing not only defensive, but also offensive strategies of warfare in this, relatively new, combat area. The United States, for example, exercise the right to respond to a cyberattack with all available conventional weapons. Because key actors in the information battlefield are precisely the most influential forces in the world and often at the disposal of nuclear arsenals, such as the US, Russia or China, it is crucial to clearly set self-determination boundaries against cyber attacks on national databases and security systems within the framework of international law (Kulesza, 2009). This, of course, further complicates relations in the international arena, poses new challenges to experts in international war and humanitarian law and raises issues of international legislative harmonization and, in general, the theory of just war, in all three aspects.

It is important to point out here that in the formal diplomatic context there are significant differences in the way individual states treat cyber issues, as is often the case in the policies of different states. Some countries, such as China and Russia, do not even use the term cybersecurity in conventional usage, but operate with the term "information security", while in the USA, the term "cybersecurity" is largely established. The choice of words is not just a matter of semantic demarcation, it rather reflects national priorities and political implications.

Unlike the United States, Russia and China are predominantly focused on the control and security of content available to their citizens. Their focus is almost exclusively on their own internal context. In contrast, security issues are about network protection, connectivity, and various aspects of communication systems, rather than controlling the content available to citizens. None of the above provides an answer to the question "what is cybersecurity" nor does it provide insight into its constituent elements. All this leads to one paradox: on the one hand, cyberspace is now firmly established as a new domain of high politics, and almost all countries express concern about uncertainty in the cyberdomain. We have not yet fully mapped the building blocks of this new domain nor its full implications in the context of national security (Choucri et al., 2012).

A. The digital transformation of the Covid-19 era

The Covid-19 outbreak and the subsequent lockdown dramatically changed the behaviour of billions of people across the world who switched to the digital space. In a matter of weeks, the restricted movement of people shifted our work, connecting and entertainment to online. With the rise of social distancing, we have been directed to our devises for almost any activity, which has consequently increased our vulnerability from all forms of cyberattacks. It might be argued that the coronavirus outbreak accelerated the inevitable digital transformation of modern society around the world (Kovar, 2020).On the global level, authorities such as the World Health Organisation (WHO) and China's National Health Commission (NHC) are using digital systems to spread and collect information about the nature and magnitude of the virus, educate the public on how to prevent transmissions and instruct on what to do if infected. Governments are using high speed telecommunications facilities to securely issue travel advice to their citizens home and abroad (Okereafor, Adebola, 2020). Companies have switched to remote work, in a struggle to mitigate the financial and operational outcomes in a climate of crisis thus making employees more susceptible to social engeenering attacks.

Amid the uncertainity about the progress of the outbreak, people are constantly in search of daily updates on the virus as well as the financial implications of the pandemic. In the short term, it is evident that internet users will continue to heavily rely on digital resources in order to get informed on how to protect themselves and better understand the situation. The trend of increased internet usage will continue until the vaccine is widely spread and a reasonable control of the pandemic is obtained. This high degree of dependence upon Internet-connected devices has already resulted in the rise of cyberattacks, and certainly will require enhanced cyberdefence measures from local, national, and global political, business, technology and cyber leaders (Morgan, 2020).

B. The impact of Covid-19 on cybersecurity

Cybercriminals thrive on chaos, whether it's real or perceived (Morgan, 2020) and the recent pandemic has offered cyberattackers unique opportunities to leverage existing attack tactics, techniques and procedures to exploit new opportunities (ECHO network of cybersecurity centres, 2020). This is confirmed also by the Interpol Secretary General in his statetement noting that "cybercriminals are developing and boosting their attacks at an alarming pace, exploiting the fear and uncertainty caused by the unstable social and economic situation created by Covid-19" (INTERPOL, 2020). It seems that the world is not faced only with a biological, but also a cyber pandemic. The desire for the latest facts on the virus has led to Internet search engines being overwhelmed with keywords such as coronavirus, Covid-19, corona, Wuhan virus, and other related keywords.

The increase in internet network traffic, particularly in regard to obtaining updated information, has favoured the spreading of malicious codes in disguise of authentic Covid-19 information. Based on the Interpol assessment of the cybercrime landscape in relation to the coronavirus pandemic, there are five key Covid-19 inflicted cyberthreats: online scams and pishing, disruptive malware (ransomware and DDoS), data harvesting malware, malicious domains and misinformation (INTERPOL, 2020). Highly concerning is the data on the shift in targets from individual to govenments and critical health infrastructure. In financial terms, it is predicted that global cybercrime damages will reach $6 Trillion Annually by 2021, up from $3 trillion in 2015 (Morgan, 2020). Governments are prone to cyberattacks by nation state supported hackers' group, which aim is to disrupt another nation state, for instance by spreading disinformation to influence the trust between citizens and their national and supra-national governmental institutions (ECHO network of cybersecurity centres, 2020). By weakening the trust between citizens and state authorities during the pandemic, hackers jeopardise effective crisis management and the return to a recovery phase. The new reality has highlighted the urge for cross border and inter-sectoral cyberdefense, taking into consideration the multifaceted nature of cyberthreats. The vulnerabilities of the system become highly prone to be exploited by the cybercriminals, including cyberterrorism, where the hospital, health-security, logistics and related supplies platforms can be breached and disrupted (UNODC, 2020).

C. Cyberterrorism as a transnational threat

Since the global nature of the threat defines protection standards around the world, it matters little whether an individual state or alliance has improved its cybersecurity and being ahead of others in doing so. Formally, the intensive efforts of states such as Canada, USA, United Kingdom, Singapore, Israel and others are very good, but as long as unverified data can flow from other states with little or no cybersecurity, the entire global system remains in conflict with threats with which it is faced. Technology always creates a new area of dependence and new benefits come with new risks. It is easy to give advice on many elements of cybersecurity, but to put together a mosaic requires a professional vision that goes beyond the technology itself and its processes (Kovačević, 2015). In the context of cybersecurity, special attention of the international community is drawn to cyberterrorism, as a transnational threat in worrying expansion and the most dangerous form of cybercrime. There is still no generally accepted definition of cyberterrorism. In technologically advanced countries, such as the United States, there is a fear that a combination of traditional and cyberterrorism could occur: therefore, that a traditional terrorist attack, such as planting an explosive device in the subway, would be accompanied by a cyberattack aimed at to disable communication between security and rescue services. This would cause enormous fear and panic among the civilian population. In that way, the damage would be maximized, thus increasing the possibility of terrorists to achieve their political goal (Putnik, 2017).

The fact is that terrorists have long seen all the advantages of cyberspace - speed of communication, ease of hiding, reduced ability to intercept communication and control cash flows in cryptocurrencies by security services, etc. Terrorists abuse cyberspace in a number of different ways: to recruit new members, to communicate and coordinate with each other, to raise funds, to spread propaganda, to identify future targets of attack, and to train their members. They are fully aware of the benefits offered by cyberspace and use this technology to facilitate attack planning and execution. For information economics, computers and computer networks form the backbone of the system that is commanded, managed and controlled. These activities should be distinguished from cyberterrorism, which by its nature is a different phenomenology and refers to the execution of cyberattacks by terrorist groups in the cyberspace. It is the type of attack that aims to cause material damage, including human losses, as well as to provoke panic among the civilian population, so that terrorists achieve a certain political or ideological goal (Putnik, 2017). Since the division of labor has reached a level of unpredictable complexity, the costliest disaster that can occur in these economies is the communication gap, which would result in certain specialized segments of divided labor falling out of synchronization. That is why communication methods which are often used are relatively inconspicuously protected by themselves or those that do not seem protected at all. This is very often a struggle at the level of who is bolder, more inventive, even no matter what technology he uses (Pejović, 2016).

III. CONCLUSION

The Covid-19 pandemic has highly exposed the vulnerability not only of individuals, but also governments from all kinds of cyberattacks. In light of the "new normal", a practical solution to the burning problem of the legal qualification of an attack on state sovereignty conducted using the Internet must initiate an international debate on the application of traditional principles of state responsibility for this new category of threats to international peace and security. In the context of statements made by national authorities from countries that are often the subject of cyber attacks (i.e. enabling a nuclear response to attacks in cyberspace), such a debate seems essential. In particular, there is a need for an international consensus on the criteria that must be met by the state in order to avoid international liability for measures taken to protect sovereignty from cyberattacks.

The main goal of that agreement would be to avoid dangerous reactions from certain states in response to cyber threats to their sovereignty. Such a discussion should begin by deciding on the legal nature of cyber attacks and identifying countermeasures that would be available to the attacked states. During such a debate, the principles and conditions for permissible self-defense against cyber attacks should be formulated, as well as preventive measures, the type and manner of their undertaking. Another key issue would be to establish a standard for relieving the state of any form of international responsibility for permitted activities

undertaken for protection purposes, which further raises the question of the need to adopt special provisions of national criminal law and effectively conduct criminal investigations by state authorities. An important element of any international agreement for liability for cyber attacks must also be the prescribing of a hierarchy and sequence of international jurisdiction and procedures applicable to acts carried out via Internet (Kulesza, 2008). Reaching such an agreement would make it possible to avoid further analogies in existing international regimes and the contradictions of national regulations. After all, such an international consensus can lay the groundwork for a broader and more comprehensive international agreement on the boundaries of state and cyberspace jurisdiction. Unification of the international regime for activities undertaken in cyberspace is already in the interest of some international organizations, including the UN (through the agenda of the Internet Governance Forum, IGF). It must be emphasized that without the establishment of an effective mechanism of state responsibility for attacks on the sovereignty of other states undertaken via the Internet from the territory of that state over the Internet, the worst and almost certain scenario is an autonomous interpretation of the UNC self-defense clause by each state individually, which would inevitably lead to armed conflict in the real world (Kuleza, 2009). The Internet is definitely the greatest human achievement and the highest possible form of democracy today in the true sense of the word. If dangerous side effects such as cyber terrorism grow into an insurmountable real threat to civilized society, we will have more control and less freedom as a result. Mankind should make every effort to find ways of mechanisms that will eliminate the causes and provide sufficient and necessary conditions for the Internet to become the common good of all mankind.

REFERENCES

[1]. Choucri, N., Elbait G., Madnick S. (2012). „What is Cybersecurity? Explorations in Automated Knowledge Generation“. MIT Political Science Department Research Paper no. 2012-30. https://ssrn.com/abstract=2178616 or http://dx.doi.org/10.2139/ssrn.2178616.

[2]. ECHO Network of Cybersecurity Centres (2020). „The Covid-19 Hackers Mind-set: White Paper of the ECHO Network of cybersecurity centres“. https://ec.europa.eu/digital-single-market/en/news/covid-19-hackers-mind-set-white-paper-echo-network-cybersecurity-centres

[3]. Gehrke, J. (2014). “Every American has been attacked by foreign cyber-hackers”. Washington Examiner. https://www.washingtonexaminer.com/rep-frank-wolf-every-american-has-been-attacked-by-foreign-cyber-hackers

[4]. IHS Markit (2017). New Report from IHS Markit Names Top Four Trends Driving the Internet of Things (IoT) in 2017 and Beyond. https://news.ihsmarkit.com/prviewer/release_only/slug/technology-new-report-ihs-markit-names-top-four-trends-driving-internet-things-iot-201

[5]. INTERPOL (2020). „Cybercrime: Covid-19 impact“. https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19.

[6]. INTERPOL (2020). „INTERPOL report shows alarming rate of cyberattacks during COVID-19“. https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19 .

[7]. J. Kulesza (2008). „Internet Governance and the Jurisdiction of States; Justification of the Need For an International Regulation of Cyberspace“. Global Internet Governance Academic Network (GigaNet). India.

[8]. Kovačević, Z. (2015). „Cybersecurity“, Internet mirror, 2015. http://www.ogledalo.rs/io-104-tema-broja-cyber-bezbednost/

[9]. Kovar, J. (2020). “COVID-19 Accelerating Digital Transformation: McKinsey“. https://www.crn.com/slide-shows/channel-programs/covid-19-accelerating-digital-transformation-mckinsey .

[10]. Kulesza, J. (2009). „State Responsibility for Cyberattacks on International Peace and Security“. Polish Yearbook of International Law. 2009/XXIX..

[11]. Ministry of Public Administration of Montenegro (2018). Cyber Security Strategy of Montenegro 2018-2021.

[12]. Morgan S. (2020). “Global Cybercrime Damages Predicted to Reach $6 Trillion Anyally by 2021”. Annual Cybercrime Report. https://cybersecurityventures.com/annual-cybercrime-report-2020/ .

[13]. Okereafor, K. & Adebola, O. (2020). “Tackling the cybersecurity impacts of the coronavirus outbreak as a challenge to internet safety” International Journal in IT&Engineering (IJITE). https://www.researchgate.net/publication/339727143_TACKLING_THE_CYB

[14]. Pejović M. (2016). „Internet - a safe haven for terrorists“. http://balkans.aljazeera.net/vijesti/internet-sigurno-utociste-za-teroriste

[15]. Putnik N. (2017). „Cyberspace has long been recognized as a legitimate combat area, Security SEE“. Security Magazine. Belgrade.

[16]. UNODC (2020). “UNODC-ROSA’s response to COVID-19: The LEA and Cybercrime Segment“. http://www.unodc.org/documents/southasia/UNODC_ROSA_on_Law_Enforcement_COVID_19.pdf.