Mujević, M. (2022). Synthesis of threats and risks of cyber security of Montenegro - the vulnerability aspect of information communication infrastructure, *SCIENCE International journal, 1*(1), xx-xx. doi: 10.35120/sciencej0101xx
UDK: sss

SYNTHESIS OF THREATS AND RISKS OF CYBER SECURITY OF MONTENEGRO - THE VULNERABILITY ASPECT OF INFORMATION COMMUNICATION INFRASTRUCTURE

Mersad Mujević[1*]

[1]International University in Novi Pazar, Republic of Serbia, e-mail: mersad.mujevic@uninp.edu.rs

Abstract: That there are no untouchables and that cyber threats are entering Montenegro through the big doors, is indicated by the hacker attack on the Government of Montenegro. Fortunately, the hackers did not get hold of confidential data, but their act itself caused a serious act of endangering state security, especially because they breached the system that is networked with all state bodies. It was not the first time in 2022 that hackers broke into Government IC systems and state and private companies and organizations. Experts from the IT sector have been warning about the vulnerability of the system for a long time, but not loudly enough to be taken seriously. Let's also mention the attack on Montenegro on the eve of joining NATO, where Montenegro was under increased cyber attacks, and the Ministry of Defense says that it is similar today.

Cyber is no longer the world of gamers and geeks, it is increasingly becoming a prefix for terrorism, crime, and other types of threats (Kazerić 2017). Internet trade and the use of electronic services such as e-government are also on the rise. To the global trend, almost everything that was only tangible and materialized in the real world is moving to the virtual community. This brings with it many advantages, but also disadvantages, and one of them is certainly the vulnerability of critical information and communication infrastructure and the danger of cyber attacks. In such circumstances, the issue of security partially shifts the focus to cyber, that is, cyber security. Precisely for this reason, it is necessary to take a critical look at the existing information and communication infrastructure and analyze the existing threats and risks brought by the modern, cybernetic age. The synthesis of threats and risks is necessary so that we can adequately face them and predict the difficulties that may come our way, which could have significant consequences for national security.

Keywords; cyber, critical infrastructure, hackers, cyber security.

1. INFORMATION SECURITY

When it comes to information security, there is no system, data, or completely secure. Experts like to joke that "the only information system that is truly secure is shut down, unplugged, locked in a titanium safe, buried in a concrete bunker, and surrounded by nerve gas and well-paid armed guards" (Spafford, according to Hadjina, 2009:7). There is a half-truth in every joke, and so it is with the mentioned quote about information security, which today, more than ever, is becoming a point of reference for every state, private, profit, and non-profit organization. Important information about company operations, state secrets, and confidential matters are no longer stored only in thick, old binders or safes. Today, they are located in the computer cloud, on the internal network of a particular company, on an employee's computer. The security of that data depends not only on hardware and software protection - but also largely on the security culture and the behavior of employees with that, often sensitive, data. Therefore, information security can be defined as the preservation of confidentiality, integrity – completeness, and availability - availability of data (Brnetić et al., 2013:6), which according to the Law on Information Security of Montenegro "is ensured by the application of information security measures and standards".

1.1. Information system

"All objects that contain all the company's information in some form are called an information system. An information system can be defined as the comprehensiveness of technological infrastructure, organization, people, and procedures for collecting, processing, generating, storing, transmitting, displaying, and distributing information as well as disposing of it" (Nađ and Adelberger, 2016:117).

The key element in that system is information that ceases to be data at the moment when it acquires meaning in a certain context. For example, data can be unrelated terms and numbers like 789, CIRT, and 2021, which are raw and have no meaning for the individual. When these data are interpreted, they acquire

*Corresponding author: mersad.mujevic@uninp.edu.rs

meaning for an individual, company, and/or institution. Thus, previously unrelated and insignificant data gain meaning when we say: According to CIRT data, 789 cyber attacks were recorded in Montenegro in 2021.

Support resources within an information system can be defined as resources within which information is located. These include hardware, software, networks, staff, locations, core services, and the organizational environment.

1.2. Aspects of information security

Aspects of information security are connected through the security triangle (CIA triad), which consists of confidentiality, integrity, and availability. In recent times, certain experts have added the aspects of provability, authenticity, and irrefutability to the mentioned categories (Kezerić 2017).

1.2.1. Confidentiality

When it comes to the first aspect of information security, confidentiality, refers to the preservation, that is, the protection of the secrecy of data and the impossibility of unauthorized persons accessing that data. Threats to the violation of data confidentiality are different, and the most common are hacking, masking, unauthorized user activity, unprotected file downloads, Trojan horses, and the like (Juran, 2012:18). "Trust attacks are attempts to break into a computer or network monitor activities or extract system information or user data. A criminal who steals a bank card or a spy who steals the design of an airplane commits an attack on trust, but the consequences of financial fraud or espionage are different" (Singer and Friedman, 2014:70). Methods of preserving data confidentiality are the use of access control and encryption methods. In the case of data access control, the point is to limit access to data marked as classified or secret through the principles of physical or logical security, and that only authorized persons can access them, while others, through physical or logical control, are denied access to that data (Kezerić 2017).

1.2.2 Integrity

Brnetić et al. (2013:6) define integrity as "protecting the existence, accuracy, and completeness of information as well as process methods". Integrity or completeness as an aspect of the security triangle refers to the fact that data/information must remain unaltered, complete, and accurate. In other words, when processing data and information, they must not be modified or changed without authorization from authorized persons.

1.2.3. Availability

To fulfill the condition of availability, data and information must be timely available and accessible to authorized users whenever there is a need for it. "Availability attacks are those that defend access to a network, either by overwhelming it with traffic or denying access or even taking it off the network and even physically shutting down virtual processes that depend on it" (Singer and Friedman, 2014:70).

1.3. Informational vs. IT security

The areas of information security specified in the Law on Information Security of Montenegro are security checks, data security, physical security, information system security, and business cooperation security. As is evident from that division, information security covers a much wider area than IT/computer security, security which mainly covers only technical parts of security. As Vuković (2012:23) concludes, "information security is only one part of information security that deals with technological protection (eg antiviruses, encryption, etc.). However, IT security does not cover e.g. managing people who are often a very big source of risk".

1.4. Information security vs. cyber security

I have already defined information security. But what does it have to do with the term cyber (cybernetic) security, which is so popular today? The point is very simple - since most information today is in digital form, information and cyber security can be considered almost synonymous. The definition of cyber security stated in the Dutch Cyber Security Strategy from 2011, and referred to by Košutić (2012:24), states that cyber security means being free from danger or damage caused by interruption, disruption, or failure of information and communication technologies or abuse of ICT a. As they further state, the damage caused by a cyber attack can consist of "limiting the availability and reliability of ICT, violating the confidentiality of the information stored in ICT or damaging the integrity of that information" (Dutch Ministry of Security and Justice, 2011, according to Košutić, 2012: 24). So, in the aforementioned

definition of cyber security, we can see all three aspects of information security, that is, the security triad. "Cyber security is 95% of information security" (Košutić, 2012:26). As the only difference between them, Košutić (2012:26) cites the fact that information security includes information security in the matter of non-digital media, that is, information security in its traditional form. On the other hand, cyber security focuses exclusively on the security of information in digital form.

1.5. "Myths" about cyber security

In today's world, cyber security is a large and indispensable part of information security and will be considered as such in the continuation of this work. However, cyber security does not "revolve" only around new technologies and is not a one-time process, which is the most common myth associated with it. Technology is only one element of a successful information security policy, but alongside it are people and processes, the importance of which should not be ignored (Klaić, 2010: 1). This is precisely why Košutić (2012) warns of six prevailing myths when it comes to cyber security, especially in modern companies.

These are the following myths:
1. Everything revolves around ICT,
2. Cyber security is not a problem of top management - they have nothing to do with it,
3. Most (future) investments in cyber security will be in technology,
4. There is no return on investment in security,
5. Cybersecurity is a one-time project,
6. The myth of documentation.

2. THREATS TO INFORMATION SECURITY

Different authors define threats to information and cyber security differently. For example, Košutić (2012:12) classifies threats as natural disasters, external malicious attacks, internal attacks, malfunctions, and unintentional human errors. They are classified by Hadjina (2009:11), who claims that there are four general types of threats in terms of computer/information systems:

- natural threats,
- unintentional threats (accidents),
- intentional active human attacks i
- deliberate passive human attacks.

2.1. Difference between risk, threat, and vulnerability

Before looking at the catalog of the tethe at it is necessary to specify the difference between risk, threat, and vulnerability. Those three terms are defined in the ISO/IEC 27001:2005 and ISO/IEC 17799:2005 standards, and they are cited by Klaić (2010:2): "Risk is a combination of the probability of an event and its consequences." A threat is a potential cause of an unwanted incident that can harm a system or organization, and a vulnerability is a weakness of a resource or group of resources that can be exploited by a threat". Therefore, the risk is always present, and the threat is realized if it takes advantage of the weakness, that is, the vulnerability of a system, and it can cause damage and cause disastrous effects to the system (Kezerić 2017).

2.2. Mapping cyber threats

The research team that sought to map EU cyber security threats in the study Cyber Security in the EU and Beyond: Exploring Threats and Policy Responses, commissioned by the European Parliament, states that there is no standard or universally accepted definition of cyber security, but that threats can be reflected actors, tools and types of threats and potential targets. Threat actors can be states, profit-motivated criminals, hacktivists, and extremists. As threat tools, they cite malware and its variants, such as banking (trojan), ransomware, point-of-sale malware, botnets, and exploits (Kezerić 2017).

2.3. Categories of malicious attacks

Vuković (2012:17) divides malicious cyber activities into:

- cybercrime,
- cyber espionage,
- cyber terrorism and
- cyber warfare.

This division can be added in recent times, especially in the widespread form of hybrid war. Considering the goal, attacks can be aimed at data or surveillance systems (Vuković, 2012:17). When an attack is aimed at data, its goal is to steal or destroy data using various tools (eg, DDoS attack) and thus sabotage an individual, company or institution, i.e. their information assets. Another type of attack is aimed at surveillance systems, whose goal is to penetrate facilities that are designated as critical infrastructure and that are necessary for the normal functioning of society and life. The boundaries between individual forms of malicious activity are sometimes very thin and intertwined. In his work, Vuković (2012:18) cites a good example of Lech J. Janczewski and Andrew M. Kolarik, who compare cyber attacks to breaking into a hospital database. According to them, if someone breaks into that database and prescribes medicine to a patient who is allergic to it, he will die. It is about cyber murder, that is, a criminal act committed using computer technology, which can be interpreted as a form of cybercrime. If, after such an act, the same attacker announces to the public that this is just the beginning and that in achieving his goals he is ready to commit more such and similar (mis)deeds, (Kezerić 2017) then it is cyber terrorism. At the same time, the cyber-terrorist will very likely try to blackmail e.g. the government of a country, stating the conditions under which they will stop their criminal activities. If the cybercriminal/terrorist is an agent of the opposing structures, then it is cyber warfare.

DDoS (distributed denial of service) is an attack that tries to overload a computer network so that thousands of computers try to connect to the same network at once, to make it difficult or impossible to access a certain computer network and/or page. Cybercrime, as I have already stated, is a type of crime carried out using computer technology. This type of crime "includes fraud in the field of Internet banking and Internet fraud with credit cards, and it is estimated that with an annual growth rate of about 40% and with current earnings of about 100 billion dollars, it is the fastest growing sector of global organized crime" (Vuković, 2012:20). In the future, cybercrime will grow even more, as well as other forms of cyber (mis)deeds due to their obvious advantages. Primarily, in carrying an attack, taking down the website of NATO or some media houses, or activating a bomb with one click, you can be in a completely different part of the world, thousands of kilometers away from your target. Also, it is very likely that an ignorant and computer illiterate individual will not do such a thing and that, of course, he will not carry out the attack from his IP address and risk having armed special forces break into his apartment, but will, thanks to his knowledge and skills, make sure that he doesn't get in the way. They probably won't learn those skills in college, but unfortunately or fortunately, Google knows everything these days. Thanks to the information that the Internet (especially the dark web) abounds in, it is more likely that they will acquire the necessary knowledge on various interactive forums and Internet guides, of which there is no shortage (Kezerić 2017). In addition to cybercrime, there are also cyberespionage, cyberterrorism, cyberwar, hybrid war, etc.

2.4. Review of some cyber incidents in Montenegro and the world

Cybercrime costs global companies around six trillion dollars a year. The largest part of the attacks refers to the world of industry, where about 21.5% of companies were affected (Passeri, 2017). In second place is the world of finance with around 15.10%. What IT experts warn about is that users of social networks are increasingly at risk. The galloping global digital transformation had strong repercussions on the proliferation of cybercrime on a planetary level, the article entitled "Cybercrime knows no borders" (see the site www.rtnk.me/me/dru% C5%A 1tvo/43846/cyber-security-ne-knocyberndaries). This is best illustrated by the assessment of leading economic experts that due to the expansion of information technology and the exponential growth of digital solutions, cyber-attacks have cyber-attacks the global economy of over six trillion dollars, which is twice as much as compared to 2015, with expectations that it will exceed the amount of 10.5 trillion US dollars by 2025. These were some of the data cited by the European Commission in the new Cybersecurity Strategy, which characterizes cybercrime as "the largest transfer of economic wealth in history that exceeds the scale of transnational drug trafficking."

In the last few years, Montenegro has faced an increase in cyber-attacks and crimes in the field of high-tech crime. Criminal offenses related to identity theft, computer fraud, account theft, ransomware, and violation of intellectual property rights are a threat, and criminal offenses of child pornography

are increasingly present, i.e. dissemination of content about sexual abuse of children. This is written in the Risk Assessment of Serious and Organized Crime (SOCTA 2022) - a document prepared by an interdepartmental team including representatives of the security sector and the prosecution, the Government of Montenegro - Bureau for Operational Coordination (2021), "Assessment of the Risk of Serious and Organized Crime in Montenegro", (see website www.gov.me).

The authorities conclude that there is a widespread use of online platforms, primarily social networks, to spread hate speech and threats, cause panic, and spread false news and misinformation: "Both individually or in smaller groups, as well as in a very organized manner." Last year, the Montenegrin police handled 672 cases in the field of high-tech crime.

Of that number, 21 attacks on websites, 75 frauds via the Internet, 86 misuse of profiles on social networks, nine inappropriate content, and 430 malware were reported to them. In the same period, 51 cases of harassment, blackmail, and identity theft were reported to them.

"The most common forms of crime are related to abuse of profiles on social networks in the form of threats, false identity, and the like, where the attacker takes control of the victim's user profiles on social networks and leaves inappropriate content in the name of the owner, all with the aim of compromise the owner of the profile," it says. document.

Officials add that among the most common forms of cybercrime are the publication of inappropriate content on the Internet, including material related to minors, and the spread of malware, including malicious blackmail programs, i.e. ransomware, the article "SOCTA 2022: Cybercrime is growing, the sharing of videos of sexual abuse of children is increasingly present (see the website www.vijesti.me/vijesti/crna-hronika/603933/socta-2022-is growing-cyber-security-all-more- sharing-videos-of-sexual-abuse-of-children). Cybercrime is growing and its presence is increasing. This means that viruses encrypt data on the infected computer and the attacker asks the victim to pay a certain amount of money to a certain account, to get the key for the encrypted data.

Among the most common attacks are DDoS attacks on the information systems of state bodies and legal entities, on the websites and portals of the Government, the websites of media companies and political parties, as well as fraudulent electronic mail and financial fraud.

2.4.1. Previous activities in the cyberspace of Montenegro

According to the data of the Digital Forensic Center (DFC) from Podgorica, the most common hacker attacks in Montenegro took place in 2017 at the time of Montenegro's accession to the NATO alliance and on the day of the parliamentary elections in 2016. During three months of 2017, government services were compromised and state institutions as well as some pro-government media. "At the time, the Montenegrin Ministry of Defense reported that it was the target of a "phishing attack", through emails that came from the EU and NATO with attachments, and which allowed hackers to install Gamefish malware on the computers of the Ministry of Defense," the DFC states. clarifying that these are methods used by the APT28 group (Advanced Persistent Threat 28, known as Fancy Bear). A gamefish is a trojan (virus) that offers a hacker broad access to a target computer, including data exfiltration, log access, and other surveillance capabilities. US intelligence has further indicated that the APT28 group is linked to the Russian military intelligence service GRU. On the day of the parliamentary elections on October 16, 2016, Montenegro faced frequent DDoS attacks, which targeted websites of state institutions, pro-NATO and pro-EU political parties, civil society websites, and election observers. Through these efforts, news websites and some political parties were taken down. After a series of attacks in early 2017, Montenegro sought the help of NATO and Great Britain, which helped to successfully repulse two attacks at the end of the same year. Due to these events, at the beginning of October 2019, members of the American Cyber Command arrived in Podgorica, of investigating signs of Russian penetration into the networks of the Montenegrin government, and also to create an insight into the opponent's cyber threats to meet the upcoming American and Montenegrin elections in 2020. year, the article entitled "FBI and ANSSI cyber experts completed the mission in Montenegro, forensic results are expected" see the website (https://dnevno.me/Dru%C5%A1tvo/-/fbi-i-anssi-sajber-strucnjaci- completed-mission-in-Montenegro-expected-forensics-results-22-09-2022-07-32-15). Based on the already mentioned data, we can conclude that the consequences of cybercrime, which does not bypass Montenegro, are severe and far-reaching, both in financial and political terms. It is official data that in the previous five-year period, more than 2,600 cyber attacks were recorded in Montenegro.

Table 1.
The number of different forms of cybercrime by year

Year	Attack on websites and IS	Internet scams	Abuse of profiles on social networks	Inappropriate content on the Internet	Malware	Others (harassment, blackmail, identity theft...)	In total
2011	1	-	-	-	-	-	1
2012	3	2	-	1		-	6
2013	5	3	10	-	1	3	22
2014	5	6	20	5		6	42
2015	6	17	37	19	17	36	132
2016	18	20	36	14	50	25	163
2017	91	18	34	9	368	12	532
2018	13	68	50	6	363	37	537
2019	19	70	79	11	387	38	604
2020	25	84	90	15	383	44	641
2021	21	75	86	9	430	51	672

3. CRITICAL INFRASTRUCTURE

Hacking websites, stealing data from bank cards, intrusions into computers and e-mails, viruses, worms... In the world we live in, these have all become common terms that people more or less encounter daily basis, but they are generally no longer surprised- because they are aware that sooner or later they can become a victim of such an attack. However, the thought of the possibility of the breakdown of the power system, the hacking of airplanes and pacemakers, or the complete interruption of communications, is not so present in the mainstream and public discourse. Such things still seem to most people to be reserved for movies or science fiction, while security experts and governments of most countries are seriously concerned about the real possibility of such scenarios. Blunden (2010:11, Kovačević, 2014:97) rightly describes the consequences of (cyber) attacks on critical infrastructure, that is, SCADA systems on which a large number of plants that are part of that infrastructure rest, as a cyber Katrina, stating that "a successful cyber - the attack on the networks that manage the vital infrastructure turned the whole of America into one big Saint Louis after Hurricane Katrina". Montenegro could feel only a small part of such a situation when in the middle of 2022, the Government's website crashed and e-mail communication was interrupted. "As a consequence of that event, there were significant negative effects such as the complete unavailability of all government services, the communication services of the PIO Fund, the Health Insurance Fund, the Employment Office, the Tax and Customs Administration, and most other services that rely on telecommunication connection". It was a case of classic system hacking, and this example pointed out the weaknesses of the critical (information) infrastructure and the need for better protection.

Montenegro adopted the Law on Designation and Protection of Critical Infrastructure in December 2019. As national critical infrastructure, the mentioned Law recognizes "systems, networks, facilities, i.e. their parts located on the territory of Montenegro, the interruption of their functioning, i.e. the interruption of the supply of goods or services via those systems, networks, facilities, i.e. their parts can have serious consequences for national security, health, and life of people, property, environment, citizens' safety, economic stability, i.e. performance of activities of public interest (Kezerić 2017). The regulation that should have been passed 12 months after the law came into force has still not been passed, it should prescribe sectoral criteria for determining critical infrastructure in the fields of energy, transport, water supply, health, finance, electronic communications, and information and communication technologies, protection environment and the functioning of state bodies and other binding norms of behavior in critical situations and the aspect of protection thereof.

3.1. Critical information infrastructure

Information infrastructure can be defined as "a combination of computer and communication systems that serve as the basic infrastructure of public bodies, industry, and economy. Critical infrastructures such as the transportation and distribution of electricity necessarily depend on telecommunications,

public telephone networks, the Internet, terrestrial and satellite wireless networks, and related computer resources for information management, communication, and control" (Brnetić et al., 2013:6). It is precisely this interdependence that makes systems, that is, infrastructure, the most critical and the most vulnerable. The two most connected systems in this sense are the electricity system, on which all other infrastructures depend, and yet it depends on the communication system and vice versa. Thus, "an outage of a hydropower plant or thermal power plant will not only hurt the energy sector, but also on the information, telecommunications, economic, financial and a whole range of service activities, but the reverse is also true" (Matika, 2009:51). Perhaps the biggest problem facing the critical infrastructure system today is asymmetric threats, which include cyber threats, and which, as stated by Klaić and Perešin (2012: 337), are very difficult to predict analytically and predict, which is why it is difficult to develop mechanisms their protection. In Montenegro, the sectoral criteria in the field of electronic communications and ICT are - infrastructure damage that causes the inability to function of the ICT system that supports key functions in Montenegro, and which relates to ensuring the operation of one of the key infrastructure sectors, the national security system, the energy system, health system and finances that lead to a drop in support lasting more than six hours. The infrastructure that can be determined as critical includes: infrastructure whose serious malfunction or interruption of operation can result in the inactivity of electronic communication networks and services for a duration of at least four hours, and which supports the work of at least one sector of critical infrastructure or national security system; infrastructure whose serious malfunction or interruption may result in non-functioning of public sector electronic services for at least six hours; infrastructure whose serious malfunction or interruption may result in non-functioning of electronic communication networks and services for at least 24 hours, in the territory where more than 15,000 inhabitants are inhabited.

3.1.1. Costs of attacks on critical information infrastructure

Cyber incidents affecting critical information infrastructure are now considered global risks that can have a significant negative impact on many cities and industries in the next 10 years" (Tofan et al., 2016:4). According to the report by Tofan et al (2016:4), attacks on critical information infrastructure mostly affect the financial, ICT and energy sectors. In the report on the costs of attacks on critical information infrastructure, the authors combined a total of 17 studies, six of which refer to the EU area, and 11 to the area outside the EU. The methods used by the authors of certain studies to extract data were surveyed/ questionnaires, analysis of logs related to cyber attacks investigated by specialized security companies, and publicly published data in the media and open sources. The most common types of attacks on critical sectors are DDoS attacks and malicious programs [Kezerić]. In terms of national loss due to attacks on information infrastructure, it reaches up to 1.6% of GDP in certain European countries. Other studies mention losses from 425 thousand to 20 million euros per company per year. One study estimates that the average cost of cyber losses per company varied between 2.3 and 15 million euros in 2015, while another study estimates the economic loss to the global economy to be between 330 and 506 billion euros. The countries whose economies suffer the greatest damage due to attacks on information systems are the USA, Germany, Japan, Great Britain, Australia, and Russia. Tofan et al. (2016:5) conclude that countries tolerate malicious activity as long as it remains at an acceptable level, less than 2% of national income, and the urgency to prepare and invest in responding to a security incident usually arises only after an event with a significant impact. Also, companies lack qualified employees, and the problem is that the vast majority of organizations still do not have basic security controls implemented. At the same time, attackers are adapting and upgrading their techniques, making them even more effective, while companies struggle with old tactics.

3.1.2. The issue of protection of information communication (critical) infrastructure in Montenegro

Very little has been written about the history of critical information infrastructure in Montenegro. However, we can say from certain sources that in Montenegro, the information infrastructure was divided into civil and military components. After the 90s, such a division was abandoned, the information infrastructure was unified, and the Ministry of Information Society and Telecommunications was responsible for the complete communication network. Since the communication of state administration bodies also went through the same communication network, when public communications were privatized, security was put on the back burner.

In this sense, unprotected critical infrastructure would have a strong impact on weakening state security, and thus the economic and social well-being of the nation. Critical information infrastructure is information infrastructure that initiates multiple elements of critical infrastructure. As information systems

are largely interconnected or connected to public systems, critical information infrastructure nowadays becomes increasingly exposed, not only to failures and breakdowns- but also to various types of deliberate attacks. The basic problem from which the necessity of recognizing critical infrastructure arises is the fact that an attack on a certain critical infrastructure in itself multiplies even greater damage because a relatively small attack on one infrastructure object can have a huge impact and cause damage to a whole series of interconnected infrastructure objects.

In the information of the Government of Montenegro, it was assessed that the operational part of cyber capacity in Montenegro is not sufficiently developed to be able to guarantee adequate protection of citizens, institutions, economic entities, and business activities of investors from cyber-attacks, fraud on the Internet, cybercrime and other threats that come from cyberspace. The National Center for the Response to Computer Security Incidents in the Cyberspace of Montenegro - CIRT, at the moment, cannot provide any response to cyber-attacks because hackers have blocked them. So much for defense against cyber attacks, and if we can't blame only CIRT for this state of affairs. In the Government announcements, which contain recommendations containing preventive measures, so that citizens do not become victims of fraud and cyber attacks, the phone number to which cyber attack -should be reported is highlighted because "the site for reporting incidents is currently unavailable (www.cirt.me)". And it is unavailable because it is under cyber attacks. And CIRT's FB profile was last updated in June 2021.

It is also a fact that we were aware of the situation and our strength in cyberspace and thus at the same time the protection of critical infrastructure in the field of ICT.

One year ago, on September 12, 2021, the Government of Montenegro determined that the strengthening of national capacities for cyber security was necessary, and the difficult conditions in which the National Computer and Computer Incident Response Team (CIRT) works were recognized as a major risk. CIRT moved from the Ministry of Public Administration, Digital Society, and Media to the Directorate for the Protection of Secret Data in November last year. In the information that was discussed at one of the Government sessions at the time, it is pointed out that the Administration for Cadastre and State Property temporarily provided premises that do not meet the requirements for the work of that body ... and especially not from the aspect of the security operations center, the processing of sensitive data, and data marked with a degree of secrecy that require the provision of a specialized room for forensics and analytics with access control and monitoring. Given that the premises in which the CIRT is located do not comply with the standards, it is not possible to use the infrastructure and systems that are under special supervision and control," the explanation states, adding that this led to a situation where the functioning of this body extremely difficult, which "represents a great risk, bearing in mind the increase in threats in cyberspace".

The document states that three types of challenges facing CIRT have been identified, and they concern not only spatial- but also technical and personnel capacities.

As for technical capacities, the document mentions that- bearing in mind budget constraints, talks with the British and American embassies have been renewed to provide technical support. Both embassies also offered help through professional training. In the information, it is added that at the operational level, access to the infrastructure of the Ministry of Internal Affairs is provided for the performance of regular activities.

It is also emphasized that, although in the age of digital expansion, information technologies are positioned as a driving force for economic development, the scope for misuse of technologies is also increasing, and cyber security is seen as an inseparable and important part of the security of any organization and state.

The draft Cyber Security Strategy of Montenegro from 2022 to 2026 envisages the establishment of a new administrative body - the Agency for Cyber Security. The plan is to establish a new and sustainable body for cyber security at the national level, within which a team for responding to computer security incidents in the cyberspace of Montenegro would function. But it was not specified what the Agency's competencies would be, whether CIRT would be transformed into an Agency, whether the Agency would be independent of CIRT, the way the Agency would be financed, etc.

Therefore, new challenges require the updating of existing cyber defense mechanisms, but also the implementation of innovative responses, especially in terms of crisis management, raising the level of digital literacy and education about the importance of cyber security issues, and the protection of privacy and personal data".

The project, launched by the Ministry of Foreign Affairs of France, through the French presidency of the European Council, in partnership with the Government of Slovenia, aims to be a center for the development of cyber security capacities in the Western Balkans region. "The Western Balkan Cyber Capacity Campus (WB3C) is designed to cover two domains - the fight against cybercrime with a focus

on educating members of the security sector and holders of judicial functions for conducting investigations and prosecuting cybercrime crimes and strengthening the regional cyber defense system, from cyber hygiene to prevention and risk management, the study entitled "eGA strengthens cyber resilience of the Western Balkans" see the website (https://ega.ee/news/ega-strengthens-cyber-resilience-western-balkans). The decision to make the Regional Science and Technology Park the location of WB3C represents an unequivocal recognition of Montenegro as a credible partner by European partners on the way to accomplishing this important task of essential importance for the region".

The educational programs of the Center are implemented in cooperation with European cyber security experts, with the support of the "Balkan institute of science and innovation of the Université Côte d'Azur" (BISI), with which Montenegro, i.e. The University of Montenegro has concluded a Memorandum of Cooperation.

There is no going back to addressing virtual security and it can no longer be treated in isolation from security in the real world. This was confirmed back in 2016- when at the Warsaw Summit, cyberspace was declared as the fourth operational domain, which created the conditions for the activation of Article 5 of the NATO Founding Treaty, which allows effective defense on an equal footing with air operations, when confronting 'aggressive behavior in cyberspace on land and sea. Therefore, it is evident that the time has passed when peace and war were two differentiated concepts- because on the cyber front we face hybrid threats of destabilization such as cyber warfare and disinformation that require a wide range of defensive means.

The tension of the drama is further fueled by the fact that cybercrime is becoming more and more intrusive and sophisticated throughout the world, which logically affects the countries with the highest degree of dependence on information technologies. This trend will continue to grow in the future because it is expected that by 2025 there will be 25 billion devices connected to the Internet on a global level, which already at this moment exceeds the total number of inhabitants on the planet.

3.1.3. Spending on the protection of critical infrastructure in the world

Critical infrastructure is undergoing an unprecedented radical transformation, initiated by the rapid adoption of smart operational technologies. Cybersecurity is a growing part of that evolution. ABI Research, a consulting company that provides strategic guidance on the most impactful transformative technologies, predicts that by 2023, $125 billion will be spent on critical infrastructure protection globally, A&S Adria, "Critical Infrastructure Protection Spending $125 Billion" by 2023, (see website www.asadria.com), 2018-;. Among the biggest investors in security are manufacturers of defense systems (Lockheed Martin, BAE Systems, Harris,), industrial OEMs (Honeywell, Siemens, Airbus, Rockwell,), technology giants (IBM, Amazon, Microsoft, Verizon), and energy companies (Shell, Total,).

Three main factors initiate better digital security;

1. in sectors such as communal services, transport, and health care,
2. digital transformation and increased connectivity of operational technologies, then
3. the democratization of cyber attacks on AI and the maturing of the market for industrial and IoT security.

Connected operational technologies have enabled the optimization and greater efficiency of decades-old systems- cost reduction and significant improvement of operator operations. But on the other hand, new vulnerabilities and threats have appeared to technologies that were previously physically separated from vulnerable networks. The first specialized attacks on industrial control systems occurred more than ten years ago, and today the tools and methods of attack are available to even the most common cybercriminals. Fortunately, the cybersecurity industry is working in tandem to bridge the gap between IT and OT. As a result, security solutions for industrial control systems and the Internet of Things are rapidly maturing and becoming more available and affordable. So, even if security personnel in critical infrastructures are faced with an increasing number of threats, they also have more choice and support in terms of digital protection of their operational and information systems. Budgets for security systems are significantly higher, which is encouraging news for those sectors that have long lagged in digital security.

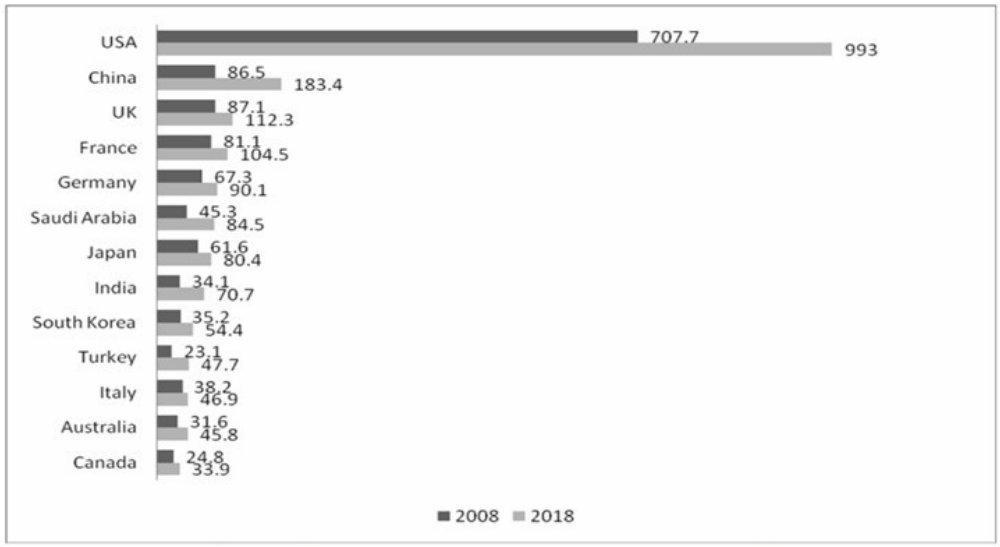
However, these positive developments face several obstacles affecting key infrastructures:

- the slowdown produced by governments about national cyber security strategies, especially in the US and the EU,
- by the continuation of resistance to the regulation of cyber security and information sharing within the sector, as well as

- by ignoring cyber security threats within the private sector, leading to his apathy towards the issue.

Many view cybersecurity as a one-time investment rather than an ongoing investment. So, even if current investments for protection are significantly higher than just a few years ago, there is still room for further investment.

Figure 1.



Slika 1 – *Potrošnja na zaštitu kritične infrastrukture ($Mr)*

As far as Montenegro is concerned, the investments are very modest, but what has been done so far inspires moderate optimism, especially if we consider the good institutional roundness and to some extent normative. Institutional capacity for critical infrastructure has been strengthened and "institutionalized" with the formation of a new sector for the coordination and protection of critical infrastructure in the Ministry of Interior. The Law on Critical Infrastructure was adopted, which prescribes the criteria for defining critical infrastructure, a disaster risk assessment study was done with a clear operational plan and clear institutional responsibilities, the Cyber Security Strategy of Montenegro from 2022 to 2026 was adopted, etc.

Also, after signing an arrangement with the EU in November 2019 for the implementation of the Joint Action Plan for the fight against terrorism in the Western Balkans, Montenegro continued to implement the planned measures and submitted its second and third reports in January and August 2021. years.

4. CONCLUSION

Based on what has been said, we can conclude that the consequences of cybercrime, which does not bypass Montenegro, are severe and far-reaching. Based on experience, we see that global cyber threats are very present in Montenegro. The statistics of the biggest global cyber threats do not differ to a great extent about Montenegrin cyberspace. Bearing in mind the results of this work, it is clear that in the future it is necessary to pay more attention to this topic, Government of Montenegro - Ministry of Information Society and Telecommunications "Analysis of threats in the cyberspace of Montenegro", 2014 (see website www.gov.me).

In the following, I will list some of the activities that must be implemented to increase the level of cyber security as well as the need for stronger protection of critical infrastructure in the ICT sector;

- Web portals of state institutions and companies from the private sector are a frequent target of hacktivists, so it is necessary to pay more attention to the proper creation of web pages and protection against possible attacks,
- One of the biggest global threats is spam, which is why it is necessary to implement antispam solutions,

- Configure the mail server to block attachments that are most often used to spread viruses,
- Tools for monitoring, updating software, removing vulnerabilities, protecting against DDoS and targeted attacks, as well as protecting mobile devices used for business purposes (see the website www.gov.me),
- Force a complex password policy,
- Create and maintain regular backups of critical systems (see website www.gov.me)
- The development and implementation of safety regulations is another key part of overall safety,
- Educate employees about the basics of cyber security and the critical infrastructure sector,
- Strengthen institutional cooperation and training regarding cyber threats and protection of critical infrastructure, etc.

When comparing the current situation regarding cyber security in Montenegro and the protection of critical infrastructure with the practice of EU countries, it is evident that there is a gap that needs to be overcome. Montenegrin society is still in the process of transition, therefore all public and private organizations are making a significant effort to quickly meet EU standards in terms of raising awareness among the population about risks and the consequences of those risks, Tempus project under the auspices of the European Commission: 544088-TEMPUS-1 -2013-1-SI-TEMPUS-JPHES, Outcomes of the project task "Comparison of practice in Montenegro with European Union standards" (see website https://ecesm.net/sites/default/files/DEV_1.3_ME.pdf).

5. LITERATURE

Mujevic, Mersad., & Korac, Safet (2020). Development of the concept of critical infrastructure protection in Montenegro - roads, experiences, roles, and responsibilities. Knowledge International Journal, 41(4), 711 - 718;
Ana-Maria, Kezerić, "Analysis of threats and risks to the cyber security of the Republic of Croatia: vulnerability of the information infrastructure", graduate thesis, University of Zagreb, 2017;
Hadjin (2009) Protection and security of information systems (teaching materials with a collection of tasks). Zagreb: Faculty of Electrical Engineering and Computing;
Brnetić, Damir, et al (2013) Criminal law-forensic protection of critical national infrastructure from IT (cyber) threats. In: Antoliš, Krunoslav (ed) New security threats and critical national infrastructure (pp. 34-45). Zagreb: Ministry of the Interior, Police Academy;
Nađ, Ivan and Adelsberger, Zdenko (2016) Information security in the context of crisis management. In: Nađ, Ivan (ed.) Days of crisis management (116-126). Velika Gorica: University of Velika Gorica;
Juran, Ana (2014) Security of information systems. Graduate work. Rijeka: Maritime Faculty in Rijeka;
Singer, Peter Warren, and Friedman, Allan (2014) Cybersecurity and Cyberwar: what everyone needs to know. New York: Oxford University Press;
Vuković, Hrvoje (2012) Cyber security and the system of combating cyber threats in the Republic of Croatia. Final specialist thesis. Zagreb: Faculty of Political Sciences;
Košutić, Dejan (2012) 9 Steps to Cybersecurity: The Manager's Information Security Strategy Manual. Zagreb: EPPS Services Ltd;
Klaić, Aleksandar (2010) Overview of the state and trends in contemporary information security policy and information security management methods. Doctoral qualification exam. Zagreb: Faculty of Electrical Engineering and Computing;
Kovačević, Božo (2014) Cyberwar – American pretext for a new cold war? Polemos: journal for interdisciplinary studies of war and peace 16(32): 91-110;
Matika, Dario (2009) Energy security, and critical infrastructure - an overview of research results. In: Matika, Dario, and Poljanec-Borić, Saša (eds) Critical infrastructure in Croatia: Towards a new system of security and protection (45-59). Zagreb: Institute for Research and Development of Defense Systems of the Ministry of Defense, Institute of Social Sciences Ivo Pilar;
Tofan, Dan; Nikolakopoulos, Theodoros; Darra, Eleni (2016) The cost of incidents affecting CIIs. Ennis.

Legal acts and norms

Cyber Security Strategy of Montenegro 2022-2026;
Law on Information Security ("Official Gazette of Montenegro", no. 14/10, 40/16, 74/20, 67/21);
Law on Designation and Protection of Critical Infrastructure ("Official Gazette of Montenegro", No. 72/2019);
Defense Strategy of Montenegro;
Disaster Risk Reduction Strategy 2018-2023;
Digital Transformation Strategy of Montenegro 2022-2026;
Disaster recovery implementation strategy (strategy for securing data in the event of a disaster for the needs of state and administrative bodies in Montenegro);
The strategy of using Open source technology;
Program for the development of information and communication technologies of the judiciary 2021-2023.

Other Internet sources

https://ccdcoe.org/cyber-security-strategy-documents. HTML
https://cert.europa.eu / static/SecurityAdvisories/2017/CERT-EU-SA2017-012.pdf
https://securelist.com /files/ 2016/11/ KL_Q3_Malware_Report_ENG.pdf
HTTPS:// securityevaluator HTTPS /hospitalhack /
www.iso27001 security.com /ISO27k_ISMS_Mandatory_documentation_checklist_release_1.docx
HTTPSHTTPSdvisera.com/27001 academy/knowledgebase/iso-27001-gap-analysis-vs-risk-assessment
www.nato.int/cps/en/natohq/official_texts_133169.htm
https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade
www.cirt.me
www.isme.me
www.yumpu.com/xx/document/view/38655723/1-pojam-information-sistema-itrevizijaba
www.zastita.info/hr/casopis/clanak/granice-kibernetícke-bojisnice-nije-lako-repoznati,22946.html
www.slobodnaevropa.org/a/crna-gora-vlada-istraga-sajber-napadi/32002798.html
https://avaz.ba/globus/region/781786/dfc-razotkrio-opasne-aktivnosti-ruske-tajne-sluzbe
www.antenam.net/politika/263510-dfc-crna-gora-u-mrezi-aktivnosti-gru
www.slobodnabosna.ba/vijest/273215/uzbuna_u_crnoj_gori_dfc_razotkrio_opasne_aktivnosti_ruske_tajne_sluzbe.html
www.scribd.com/document/580304186/strategija-sajber-bezbednosti-crne-gore-2022-2026-spredlogom-akcionog-plana-za-period-2022-2023-1
https://pubdocs.worldbank.org/en/384771604613506147/3-Energetski-sektor.pdf
https://docplayer.rs/211233602-Analiza-prietnji-i-rizika-cyber-sigurnosti-republike-hrvatske vulnerability of information - infrastructure.html
https://ne-np.facebook.com/102994798278482/posts/hakeri-blokirili-i-crnogorski-nacionalni-centar-zaodgovar-na-sajber-incidente/585724080005549
www.baltictimes.com/ega_strengthens_cyber_resilience_of_the_western_balkans_countries
www.scribd.com/document/486514599/15-94-18-12-2014-pdf