



GOVERNMENT OF MONTENEGRO
MINISTRY OF PUBLIC ADMINISTRATION

CYBER SECURITY STRATEGY OF MONTENEGRO

2018
2021



Government of Montenegro
Ministry of Public Administration

CYBER SECURITY STRATEGY OF MONTENEGRO

2018-2021

December 2017

Table of Contents

01

Introductory review	4
---------------------------	---

02

Modern risks, threats and challenges	6
--	---

Revolution of new technologies	7
Threats and risks in cyberspace	9
Other significant challenges	10

03

Retrospekt (From the first Cyber Security Strategy unitl today)	12
---	----

Defining institutional and organisational structure in the field of cyber security in the country	13
Protection of critical information infrastructure in Montenegro	14
Strengthening capacities of state law enforcement authorities	15
Incident Response	15
Defining the role of the Ministry of Defence and the Armed Forces of Montenegro in cyberspace	16
Partnership of public and private sectors	16
Raising public awareness and online protection	16

04

National organisational structure	18
---	----



05

National cyber defence 22

Cyber defence capacities	24
Centralisation of cyber expertise and resources	25
Protection of critical information infrastructure	26
Inter-institutional cooperation	28
Data protection	29
Cyber security education	30
Partnership of public and private sectors	32
Regional and international cooperation	33

06

Monitoring 34

07

Concluding review 36

Annex

Definitions and terms 40



01

Introductory review

Due to the constant growth of the number of online services that public and private sectors provide to the citizens as well as to other legal entities, safe cyberspace of Montenegro is becoming one of national priorities.

Smart phones, social media, systems for industrial production control, numerous medical devices controlled by information systems are only some of the examples of putting technology to use, or the benefits it provides.

According to estimates, there are about 8 billion of inter-connected devices in the world. It is estimated that by 2020, the number of devices would exceed 20 billion, which speaks for the degree of integration of physical systems with the computer systems, resulting in greater effectiveness, accuracy, greater economic benefits, but also more serious adverse consequences in case of a cyber attack.

Bearing in mind increasing integration of cyber and physical systems and adverse consequences which could be caused by a compromised cyber system, cyber security and its developed national, regional and international architectures play a crucial role.

The accelerated development of inter-connected, innovative technologies must also be followed by a fast development of cyber-security solutions, namely the protection from a wide spectrum of threats and that certainly represents a challenge to which all of us must respond with joint forces.

Undoubtedly, cyber security is a challenge of the modern age and, as such, not even Montene-

gro is exempt from it. We witness an increasing number of cyber incidents which affect Montenegro, through the recent ransomware campaigns, DDoS attacks against the public infrastructure, various online frauds, etc. Year after year, the number of these cyber incidents is significantly increasing.

We must be aware that the threats to the IC infrastructure which may threaten its availability, privacy and integrity may also affect the functioning of the society as a whole. Countries, international organisations, security companies, and various other entities are constantly developing and implementing new security mechanisms, however, simultaneously there is a process in which cyber criminals are inventing innovative and sophisticated techniques to bypass them.

With regard to the development of information technologies and cyber security, according to the UN report i.e. International Telecommunication Union (ITU) report called "Global Cybersecurity Index¹ 2017", Montenegro ranks 71st out of 193 member states. However, due to daily occurrence of new threats, our efforts with regard to cyber security must follow that pace as well.

¹ Global Cybersecurity Index 2017.

Link: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf

02

Modern risks, threats and challenges

Continuous advancement of information technologies and enlargement of the cyberspace to a large extent stimulates economic and social progress of every country in the world. Information security represents a common interest of the entire mankind and it refers both to the global peace and development and to the national security of all countries. However, this advantage also entails new security risks and challenges.

There are numerous risks and challenges faced by a large number of countries. The increase in the number of information systems and technologies, among other things, conditioned the setting up of new memory environments (Cloud Storage), which certainly represents a great challenge and is the subject of separate analyses. Furthermore, there is an evident increase in the number of malicious programs for mobile devices.

According to the research presented by Symantec in April 2017², about 18.4 million of malicious programs were detected in 2016, which is 105% more than in 2015 (9 million). In 2014, approximately 3.6 million pieces of malware were detected.

Revolution of new technologies

The Internet revolution carries a number of

extremely useful possibilities, so an evident huge increase in the number of users every day is no surprise.

It is interesting to note that, since the beginning of the implementation of the previous Cyber Security Strategy for Montenegro (2013), the number of internet users on a global level has increased from 2.5 billion to 3.9 billion (until June 2017)³.

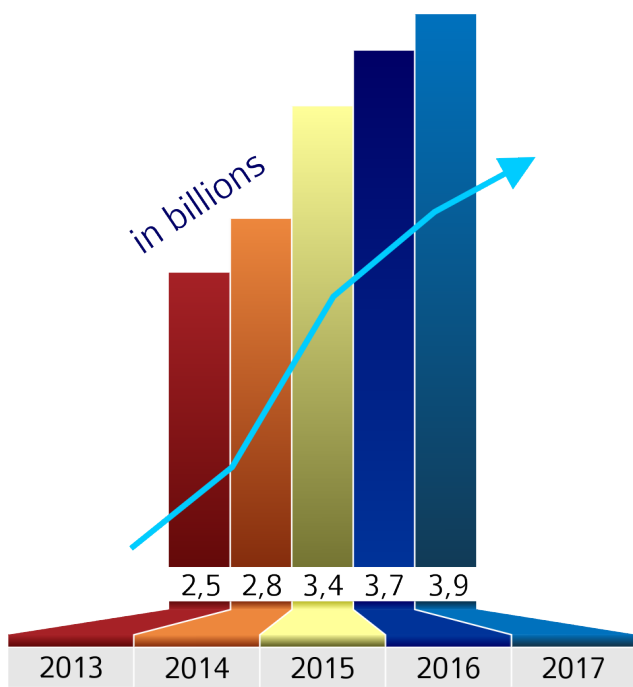
We can come across the expression “proliferation of cyber technology” in the literature. This term refers to the parsing or multiplication of technologies which, by connecting to the global network, also become a part of the cyberspace.

One of the sources of cyber risk proliferation is the Internet of Things (IoT), a term first defined by Kevin Ashton, founder of the Auto-ID Centre at the MIT, in his presentation on the new possibilities of RFID in Procter & Gamble’s supply chain in 1999.⁴

² Symantec Internet Security Report vol. 22 - <https://www.symantec.com/content/dam/symantec/docs/reports/gistr22-government-report.pdf>

³ <http://www.internetworldstats.com/emarketing.htm>

⁴ RFID Journal — “That ‘Internet of Things’ Thing”: <http://www.rfidjournal.com/articles/view?4986>



Global penetration of Internet users
in the period 2013-2017

IoT is a set of devices, vehicles, household appliances, as well as other items with built-in electronics, software, sensors, etc. connected to a shared network. Taking into account the fact

that the connecting of the aforementioned items enables unhindered communication, recording of information and data exchange, the concern in the world of informatics is quite justified. Therefore, this concept represents one of the leading security issues in the world.

The term that includes a larger domain is called the Internet of Everything (IoE) and was first defined by CISCO as a part of the 2013 study entitled "Internet of Everything Value Index"⁵.

IoE represents an intelligent network of people, processes, data and things. More accurately, it is based on IoT, adding network intelligence that enables the efficient use of telephone, video and data communications via the same network (convergence), automation or process improvement with potential synchronisation of real-time data (orchestration), as well as visibility in different systems.

On the other hand, an abundance of different options brings with it threats that can cause adverse consequences to a large extent.

*"We are entering the fourth generation of the Internet.
In the next 10 years, we will see that the competitiveness of the company will be
measured by how well they understand the IoE concept and how much they use it."*

Michael Ganser
Senior Vice President of CISCO Central Europe

According to a study presented by one of the Britain's and global leading research companies in 2017, IHS technology, more than 20 billion devices are connected via the Internet. It is estimated that by the end of 2020 there will be at least 30 billion, while by 2025 this number will exceed an incredible 75 billion.⁶

Such an expansion of devices will definitely bring about new opportunities, but will also make additional room for actions of malicious individuals or groups, because in most cases the devices are not designed in compliance with the online security standards.

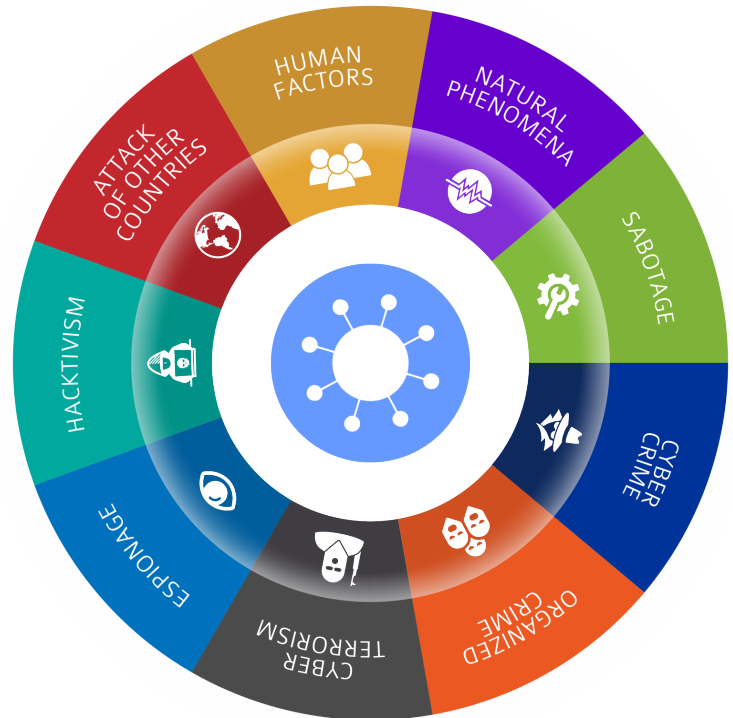
⁵ <https://newsroom.cisco.com/press-release-content?type=webcontent&articleId=1209280>

⁶ IHS Technology – IoT platforms: enabling the Internet of Things: <https://cdn.ihs.com/www/pdf/enabling-IOT.pdf>

Threats and risks in cyberspace

Taking into consideration the ultimate goal of cyber activities, threats can be classified into two basic categories:

- **cyber attacks** (attacks by other countries, hacktivism, espionage and sabotage), **cyber terrorism** and **cyber crime** (creation of terrorist organisations, attacks by individuals or groups, organised crime), **cyberwarfare**,
- risks caused by human error or natural phenomena.



Cyber attacks

Numerous activities can be listed under cyber attacks. In many cases the attacks are carried out for the purposes of espionage and sabotage.

Espionage refers to the unnoticeable tracking and collection of information and confidential data about a person or a company using different software and services, which can eventually be publicly presented, most often through media. The activities are usually carried out using a method called “backdoor”, which can be special software or be incorporated as a program code in the firmware of a network device and thus deliver information to the attacker.

Sabotage achieves certain goals, most often of political nature. In this manner, the processes of institutional work or military action are deliberately interfered with and this enables the removal or takeover of control and command. The most common examples of sabotage are carried out using botnets for DDoS/DoS attacks.

During 2016, the companies Kaspersky Lab and B2B International polled about 4,000

companies from 25 countries that were affected by some of the DDoS attacks.⁷ About 40% of the companies said they believed that the attack had been caused by their competitors, 20% blamed foreign governments and secret service organisations, while 20% suspected that the attacks had been carried out by former employees.

The second problem refers to **cyber crime** and **hacktivism**. Worldwide, there is an evident increase in the number of malicious software being distributed in different ways. The launching of such software enables stealing of sensitive data, monetary gains, loss of service and eventual destruction of data and devices.

Hacktivism is the act of hacking or breaking into a computer system, for political or social reasons.

Furthermore, internet penetration enables adequate action by perpetrators of **cyber terrorism**. Nowadays it is much easier to create terrorist organisations, smaller organised groups, or

⁷ Kaspersky Lab Finds Businesses are Unclear on How to Combat Targeted Attacks and DDoS

Link: https://usa.kaspersky.com/about/press-releases/2017_kaspersky-lab-finds-businesses-are-unclear-on-how-to-combat-targeted-attacks-and-ddos

hire individuals who, in the name of certain interests, will have considerable power to inflict as much damage as possible using modern Internet technology. In this regard, numerous attacks on critical information infrastructure of the countries are being organised, which is developing into a model of **cyberwarfare**.

The attack and/or destruction of critical information infrastructure achieves the goals of disruption or complete outage of vital state or military communications, resulting in certain consequences for the civilian population. For example, an attack on industrial control systems in the energy supply system may result in a breakdown of production and/or distribution of electricity for the population, causing numerous problems. Furthermore, the attack on information systems in the healthcare sector can cause damage to people's health, through possible modification of parameters on devices which the patients use to communicate online with the system in the healthcare institution.

In addition to the above mentioned, it should be noted that a great challenge is also the fact that nowadays online instructions for organising cyber attacks using the "*know-how to launch cyber attacks*" model are widely available.

Risks caused by natural disasters or human error

In its "2014 Cyber Security Intelligence Index" research report, IBM's presented a highly intriguing piece of information saying that 95% of all security incidents were caused by the factor of human error.

Many successful attacks were carried out by attackers using human weaknesses and various forms of intimidation to turn employees into insi-

ders, who reluctantly allowed access to classified information.

Contrary to that, there are constant risks that are difficult to predict and the entire mankind struggles with them; they are caused by natural disasters, such as: earthquakes, floods, and hurricanes. Great physical damage can also be caused by fires, extremely high temperatures and lightning strikes, which can also lead to data loss.

Other significant challenges

Challenges relating to the home affairs of a country are equally significant as the risks and threats described above. More specifically, they represent one of the important prerequisites for adequate cyber protection.

A need for further investment of funds in the strengthening of resources, expertise and continuous progress in the field of proactive action within the cyberspace of Montenegro was recognised. In a large number of countries and international organisations, such as NATO and the EU, cyber security is one of the top priorities, and so this problem has also been defined in relevant strategies and concepts of cyber security.

In addition to the above mentioned, the **legal framework limitations** in this field are causing difficulties in procedure implementation. Namely, the cyber attacks on a country to be labelled as digital "armed attacks" remains a challenge. For this reason, there is a lack of adequate **international level cooperation**, while the role of international organisations is also very limited.

Inadequate **communication and cooperation between the public and private sectors** largely results in the lack of trust of citizens in institutions and companies doing business online. On the other hand, **insufficient digital li-**


teracy of end-users and failure to observe **best practices** when using a communication device is a separate challenge. The reason for the above mentioned problem is **insufficiently raised awareness among the population** about the problem of cyber security in general.

Finally, a great challenge for countries is a **small number of experts** who would be able to constantly participate in the cyber security domain and adequately implement reforms.

Following the best security practices, one of the challenges is to **clearly separate the fun-**

ctions of administration and governance of information systems from the security management function of these systems. In cases when human resources are limited, in some institutions the functions of security and administration overlap. This fact directly causes a decrease in the level of security of the system because there is no second instance control over administrators, but they themselves also perform the security function of their institution.





03

Retrospect

The Cyber Security Strategy for Montenegro 2018-2021 is a continuation of the previous strategy, whose life cycle ends at the end of 2017.

The Cyber Security Strategy for Montenegro 2018-2021 is a continuation of the previous strategy, whose life cycle ends at the end of 2017.

The starting point for the activities to be undertaken in order to define and implement the Cyber Security Strategy for Montenegro 2013-2017 was, in the legislative sense - the Law on Information Security (Official Gazette of Montenegro, No 014/10), and in the institutional sense - Directorate for Protection against Computer and Security Incidents Online (CIRT), which operated within the then Ministry of Information Society and Telecommunications, and now belongs to the newly established Ministry of Public Administration of the 41st Government of Montenegro, with the task of enabling early detection of cyber threats and incidents and adequately reacting and responding to them.

The first Cyber Security Strategy for Montenegro was adopted in 2013 for the period until 2017 and contains seven key strategic objectives:

1. Defining institutional and organisational structure in the field of cyber security in the country;
2. Protection of critical information infrastructure in Montenegro;
3. Strengthening capacities of state law enforcement authorities;
4. Incident response;
5. Defining the role of the Ministry of Defence

and the Armed Forces of Montenegro in cyberspace;

6. Partnership of public and private sectors;
7. Raising public awareness and online protection.

The implementation of the above strategic objectives was defined in more detail in two action plans for the implementation of the Strategy. The insight into the status of their implementation shows the intensive activity of the responsible authorities in fulfilling the set strategic objectives, which resulted in the successful implementation of a part of the activities identified in the action plans.

The chapter continues to describe in detail the activities undertaken in order to deliver the main strategic objectives of the Cyber Security Strategy for Montenegro 2013-2017, as well as the activities not undertaken on a satisfactory level which will be covered by the Cyber Security Strategy for Montenegro 2018-2021.

1. Defining institutional and organisational structure in the field of cyber security in the country

This strategic objective recognises the need to have a clear organisational hierarchy within the

public administration, with defined responsibilities, which will ensure effective cyber security governance in Montenegro. The following have been identified as the institutions accountable for cyber security in Montenegro:

- Ministry of Public Administration within which the national CIRT operates;
- National Security Agency;
- Ministry of Defence / Army of Montenegro;
- Ministry of Interior / Police Administration;
- Ministry of Justice;
- Ministry of Education;
- Directorate for Protection of Confidential Data.

The accompanying two-year action plan for the implementation of the Strategy envisages the formation of the Information Security Council, which was formed at the 29th Session of the Government on 08 June 2017.

Furthermore, the Cyber Security Strategy for Montenegro 2013-2017 envisages the formation of local CIRTs or appointment of contact persons in all state authorities, aimed at strengthening cyber infrastructure at the local level. A total of 31 local teams were created, in charge of cooperating with members of the national CIRT on the issues of protection against computer security incidents on the Internet.

Degree of implementation:

It is evident that cyber security is becoming increasingly important in state authorities and that the institutions have largely recognised their role in cyberspace. Further activities aimed at completing the list of local CIRTs and appointing contact persons for cyber security issues will be the subject of activities of the relevant institutions through the Action Plan 2018-2019, which will accompany the Cyber Security Strategy for Montenegro 2018-2021.

2. Protection of critical information infrastructure in Montenegro

In accordance with the task, the then Ministry of Information Society and Telecommunications of the 40th Government of Montenegro drafted the Law on Amendments to the Law on Information Security (Official Gazette of Montenegro No 040/16) defining critical information infrastructure (CII).

Critical information infrastructure consists of information systems which, if compromised or destroyed, would endanger the life, health, and safety of citizens, as well as the functioning of the country, while the performance of public interest activities depends on their proper functioning.

Upon the proposal of the then Ministry of Information Society and Telecommunications, the Government of Montenegro adopted the Methodology for selecting critical information infrastructure. Based on the Methodology and in cooperation with other relevant institutions, the Ministry of Public Administration, which inherited certain responsibilities of the former Ministry of Information Society and Telecommunications, has defined the list of critical information infrastructure in Montenegro, and the drafting of a Decree on measures for protecting CII is under way.

Degree of implementation:

The initial list of critical information infrastructure in Montenegro has been adopted, however, it should be taken into consideration that the list is to be regularly updated. After the adoption of the Decree on measures for protecting CII, it is necessary to implement it in cooperation with the owners of the CII.

3. Strengthening capacities of state law enforcement authorities

In the previous period, through legislation and strategic documents, Montenegro has followed the main standards, guidelines and recommendations of the EU and NATO regarding the cyber security capacity building.

The information security legislation has been harmonised with the EU acquis to a significant extent. In addition, in 2016, the Law on Amendments to the Law on Information Security (Official Gazette of Montenegro, No 040/16) was adopted, providing for two key activities: the formation of the Information Security Council and the protection of critical information infrastructure, which are in line with the NIS Directive (2016/1148)⁸.

In order to strengthen the capacities of state law enforcement authorities, a High-Tech Crime Group has been set up at the Ministry of Interior, and it belongs to the Section for Fighting against Organised Crime and Corruption. The said Group provides for three working positions for staff dealing with the issue of high-tech crime (classical acts of computer crime, child pornography, credit card abuse, and copyright abuse).

As of June 2013, a group for testing information technologies has been envisaged within the Forensic Centre of the Police Administration in Danilovgrad. With regard to technical capacities, in addition to computer testing tools, mobile phone testing tools were also procured.

The National Security Agency is making significant efforts aimed at creating normative and operational mechanisms for fighting against cyber crime and espionage, which, along with terrorism and organised crime, are becoming the greatest security challenges of today. The agency is working continuously and intensively

in order to strengthen cyber security organisational and technical capacities.

In order to strengthen the resilience of information systems, the ICT Service at the Ministry of Justice has carried out a series of activities in line with the tasks set out in the Strategy, which greatly reduce the vulnerability of the existing systems of the Ministry in cyberspace.

Degree of implementation:

Although the state authorities have recognised the need to strengthen their cyber security and cyber crime capacities in the previous period, it is necessary to continuously invest in further improvement of national cyber defence capacities.

4. Incident Response

The analysis of the incident reports in Montenegro, which are drafted annually by CIRT, shows an evident trend of growth in the number of reported incidents year after year, as well as an increasing degree of sophistication of the attacks themselves.

With the establishment of the national CIRT, a major step has been taken towards increasing the ability of state authorities to respond to cyber incidents affecting Montenegro.

Degree of implementation:

CIRT has been recognised as a focal point for responding to incidents in Montenegro, however, there is an evident lack of highly specialised personnel for successfully responding to this challenge. In addition to the above, in order to respond to incidents, it is also necessary to implement tasks relating to the completion of the list of local CIRTs, as well as to the trainings for

⁸ http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC

the narrow specialisation of employees from the field of cyber security.

5. Defining the role of the Ministry of Defence and the Armed Forces of Montenegro in cyberspace

The Ministry of Defence (MoD) and the Armed Forces of Montenegro (AFoM) are fully responsible for the cyberspace created within MoD and AFoM and they cooperate with the national CIRT in Montenegro's cyberspace protection.

NATO targets (E 6202 N) have been adopted, defining the capacities that MoD and AFoM should develop in the next 2 to 5 year period.

Degree of implementation:

MoD and AFoM have a clear vision of their role in cyberspace. The role of MoD and AFoM will be further strengthened through the additional activities planned for the upcoming period.

6. Partnership of public and private sectors

A large part of critical information infrastructure belongs to the private sector. Therefore it is necessary to clearly define cooperation with the private sector in the field of cyber security.

With regard to the private sector, seven CIRTs were created within the companies Crnogorski Telekom, Telenor, M:tel, Wireless Montenegro, Telemach, M-kabl and Societe Generale Montenegro Bank.

One of the best examples of cooperation with the private sector is the activities undertaken

to organise joint promotional campaigns on the protection of children in cyberspace and the safe use of the Internet.

Bearing in mind that CIRT recognised malware as one of the biggest threats in Montenegrin cyberspace, a pilot project was launched on 4 November 2016, in cooperation with the Agency for Electronic Communications and Postal Services (EKIP) and Internet providers in Montenegro.

The project was aimed at identifying infected computers as well as undertaking activities in order to recover from the consequences. The above was done in cooperation with EKIP and the Internet providers operating in Montenegro. In November 2016, joint meetings were held on this topic, and the test stage of the project was carried out.

Degree of implementation:

Evident progress has been made in terms of strengthening cooperation with the private sector. Bearing in mind the significance of having a partnership of public and private sectors, it has been recognised as a priority by the Cyber Security Strategy for Montenegro 2018-2021.

7. Raising public awareness and online protection

In line with the task from the Strategy, the Ministry of Public Administration has actively worked on educating citizens through the leading of various promotional campaigns with a special focus on the protection of children on the Internet⁹. Additionally, in 2017, the Ministry of Public Administration decided to organise a special segment within INFOFEST dealing with the issue of cyber security.

⁹ <https://www.telenor.me/cg/o-telenoru/o-nama/drustvena-odgovornost/odgovorno-poslovanje/surfui-pametno/>;
http://www.cirt.me/O_Nama/prijavisadrzaj

The Human Resources Administration also included a training for civil servants and employees on the topic of cyber security in its regular training program, which is being carried out in cooperation with the Ministry of Public Administration. So far, 350 civil servants and state employees have completed the training.

In addition to this, a highly specialised training was conducted for staff members working on cyber security tasks. Some of the most important trainings were conducted in cooperation with NATO: M6-108 Network Security Course and M6-109 Network Vulnerability Assessment and

Risk Mitigation Course, attended by 30 civil servants each.

Degree of implementation:

This strategic objective has been implemented to a significant extent. However, given the speed of the development of information technologies, the increasing number of threats in the cyber space, as well as the lack of highly specialised personnel, this activity needs to be continuously implemented.

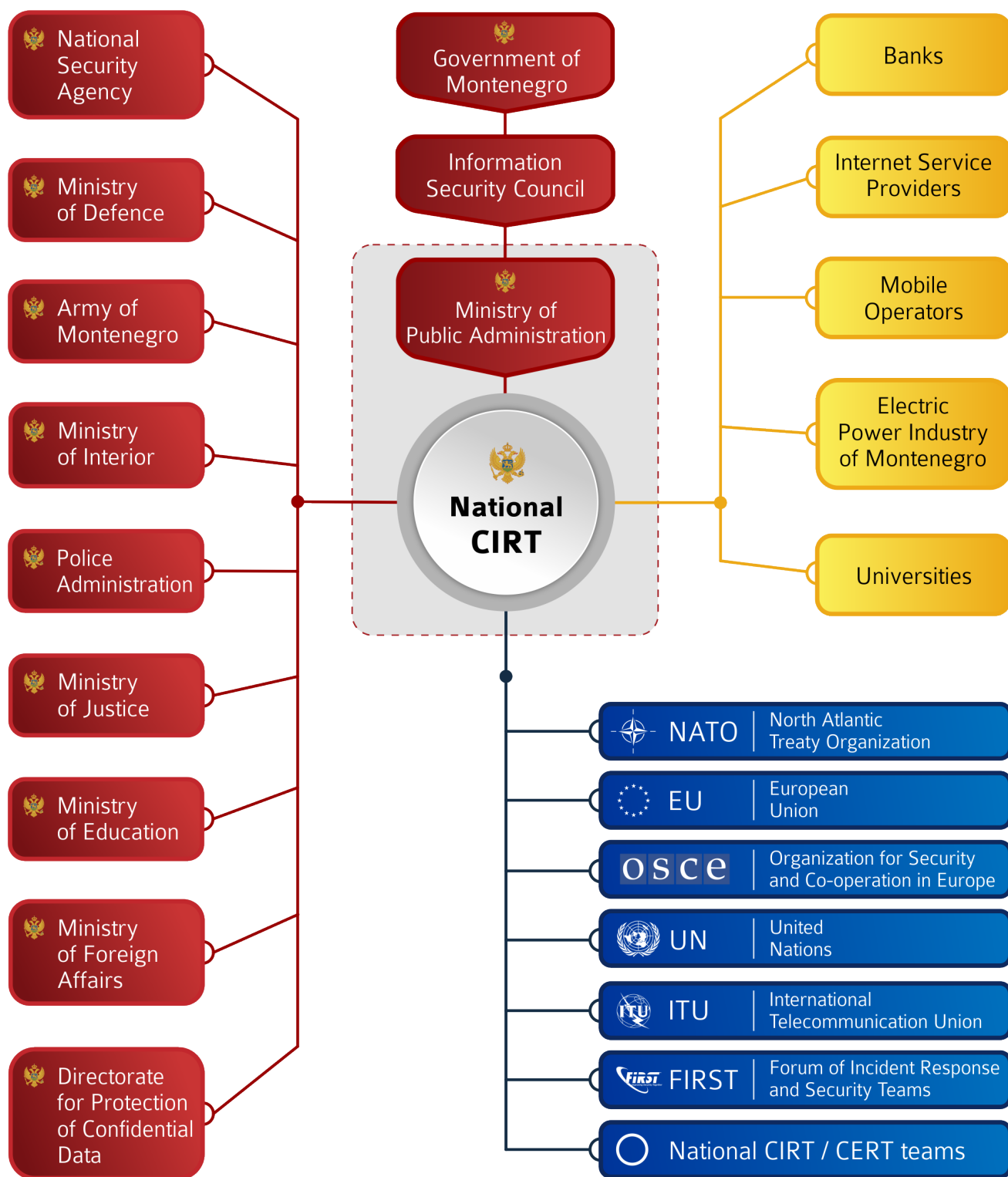




04

National organisational structure

National cyber security structure of Montenegro



It is necessary to have a good organisational hierarchy within the state administration, that will ensure the most efficient and long-term sustainable provision of adequate cyber security governance in Montenegro.

In line with the task of providing early detection of cyber threats and incidents and adequately reacting and responding to them, the Directorate for Protection against Computer and Security Incidents Online (CIRT) was formed in 2012.

CIRT is the central body for the coordination of prevention and protection against computer security incidents on the Internet and other security risks to information systems for the territory of Montenegro. In accordance with its responsibilities, CIRT acts:

- In a preventive manner - through education, raising

awareness, providing useful information and advice on internet security, and

- In a reactive manner - through analysis and conducting detailed investigations in case of online incidents at the national level.

In addition to this, CIRT carries out activities to establish and promote partner relations both at the national level (with relevant authorities, private sector partners, and academic community), and the international level, in order to respond to cyber threats in a better and more efficient manner.

The analysis of the incident reports in Montenegro, which are drafted annually by CIRT, records a trend of growth in the number of reported incidents year after year, as well as a degree of sophistication of the attacks themselves.

Year	Attacks on websites and IS	Online frauds	Abuse of social profiles	Inappropriate content online	Malware	Other
2013	5	3	10	-	1	3
2014	5	6	20	5	-	6
2015	6	17	37	19	17	36
2016	18	20	36	14	50	25
2017 (until Sept 1)	90	13	25	4	245	8
TOTAL	124	59	128	42	313	78

Statistics by year and type of attack

In accordance with the Law on Amendments to the Law on Information Security (Official Gazette of Montenegro, No 40/2016) the Information Security Council was formed on August 1, 2017 (Official Gazette of Montenegro, No 48/2017), thus providing a national parent organisation to advise the Government of Montenegro on all important issues in this field.

The Council's tasks are to:

- inform the Government of Montenegro on all important issues related to cyber security;
- monitor the implementation of the Cyber Security

Strategy for Montenegro and the action plans for its implementation;

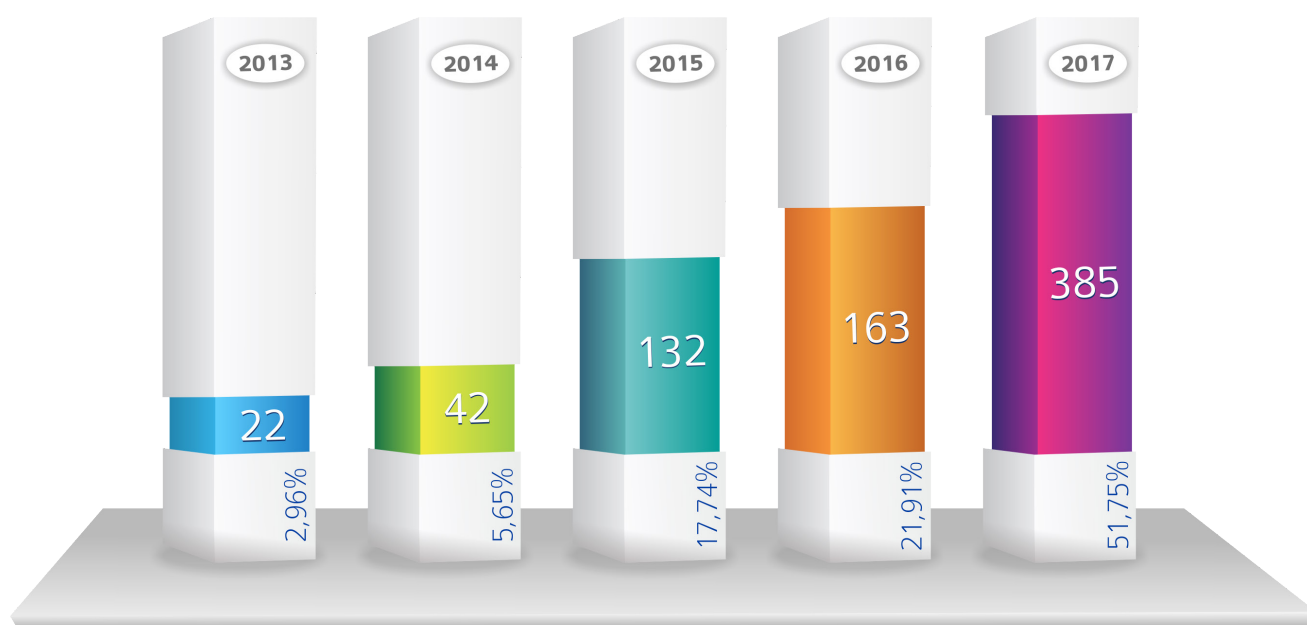
- monitor and coordinate activities in the field of cyber security;
- propose measures for harmonisation of the legislative and administrative frameworks in order to improve the cyber security of Montenegro;
- work to improve cooperation between state authorities and administrative bodies in the field of cyber security and coordinate their activities;
- work to improve cooperation with the private sector in the field of cyber security;
- submit its performance report to the Government of Montenegro at least once a year.

Members of the Council are representatives of the following institutions that have been identified as the institutions accountable for cyber security in Montenegro:

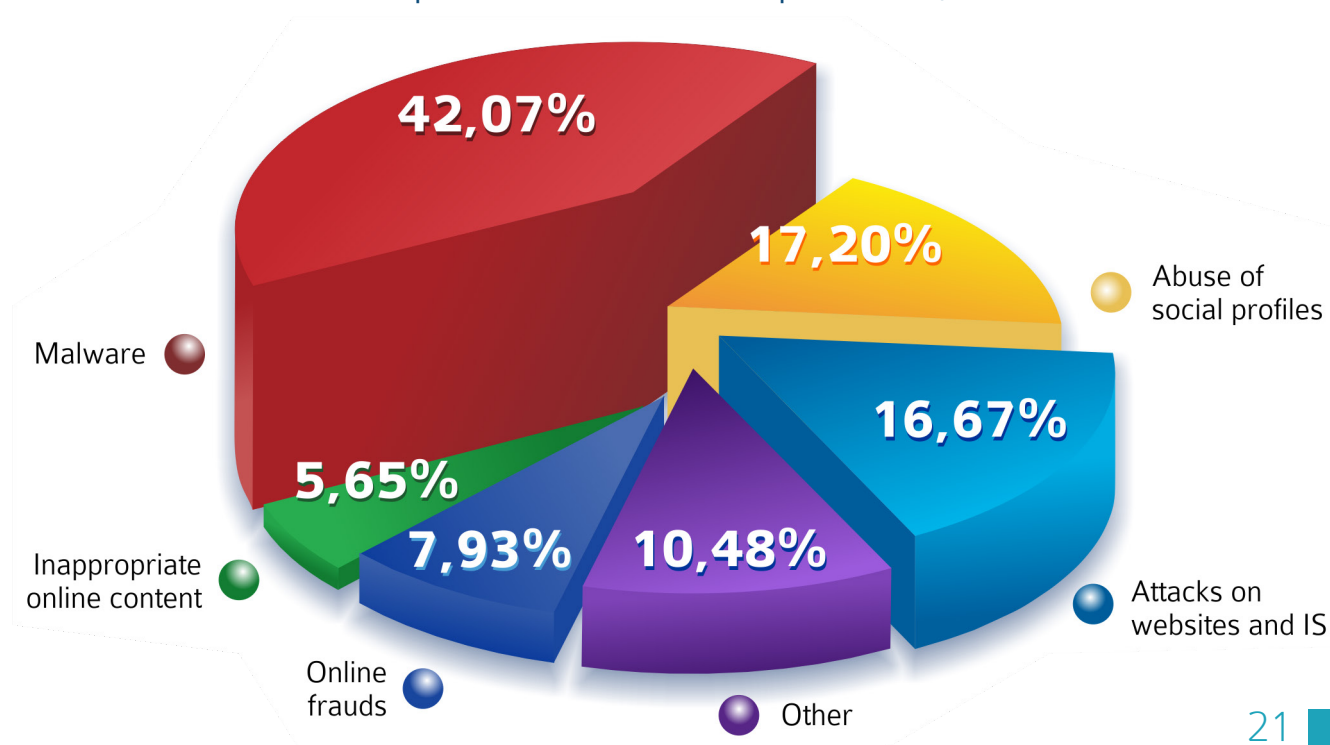
- Ministry of Public Administration,
- Ministry of Defence,


- Ministry of Interior,
- Ministry of Justice,
- National Security Agency,
- Directorate for Protection of Confidential Data.

Number of reports and percentages by year, compared to the total number of reports, for the period from 2013 to September 1, 2017



Statistics of incidents reported to the national CIRT, by type, in the period from 2013 to September 1, 2017





05

National cyber defence

The development of a national concept for cyber security should now be directed through two newly formed important factors, from the adoption and implementation of the first national cyber security strategy - accession to the NATO alliance and the opening of the negotiation Chapter 10 - Information Society.

In July 2016, the European Union adopted the Network Information Security Directive of European Parliament and of the Council 2016/1148. The goal of this Directive is a comprehensive regulation of national cyber security of the Member States. It consists of five chapters and, in order to fulfil the obligations, the Member States, shall:

- adopt a national cyber security strategy;
- define the relevant authorities in the field of cyber security;
- have at least one Computer Emergency Response Team (CERT). These teams have to cover relevant sectors and services. These teams must also have adequate resources and tools in order to fulfil their complex functions and tasks;
- regulate the security of the information systems of the owners of essential, critical services in the technical and organisational manner stipulated by the Directive;
- regulate the security of the information systems of the owners of digital services in the technical and organisational manner stipulated by the Directive;
- voluntarily use the recommended EU standards.

The extent of the differences between the EU member states regarding the protection of network and information security can be concluded from the directive itself:

„Existing capabilities are not sufficient to ensure a high level of security of network and information systems within the Union. Member States have very different levels of preparedness, which has led to fragmented approaches across the Union. This results in an unequal level of protection of consumers and businesses, and undermines the overall level of security of network and information systems within the Union.“

„National strategy on the security of network and information systems‘ means a framework providing strategic objectives and priorities on the security of network and information systems at national level.“

Pursuant to Article 7 of the NIS Directive, each Member State shall adopt a national strategy on the security of network and information systems by 9 May 2018, which may be considered as equivalent to the National Cyber Security Stra-

tegy, and six months after that Member States must complete the identification of operators of essential services. The Commission adopted an Annex on the effective application of the NIS Directive COM (2017) 476 of 4 October 2017. Furthermore, the Commission presented a proposal for the ENISA reform, which includes its permanent mandate as a reference point in the EU cyber system, and that it will ensure the implementation of the NIS Directive and the proposed Information and Communication Technology cyber security certification Framework COM (2017) 477 of 4 October 2017. For some companies that hold critical sectors, the EU's General Data Protection Regulation (EU) 2016/679 of 27 April 2016 is very important, and it will be in application as of May 2018. Companies will have to take care of the data processing of the entities from the EU due to severe penalties for non-compliance, therefore they are obliged to start adapting their business to the new requirements of the Regulation that deal with information risks, ICT security, rapid reaction to discovering threats and data breach, recovery of information and continuity of successful business.

Although the NIS Directive is not binding for Montenegro, the implementation of its recommendations would contribute to the development of a modern, efficient and European compatible national cyber security concept.

And while there could be room for discussion about the application of ENISA recommendations, when it comes to the NATO alliance, there is no dilemma for Montenegro as its full member. At the Warsaw Summit of 2016, NATO declared the cyber domain the fourth operational domain, making the effects and consequences in cyberspace equal to that within the remaining three domains: water, air and land. Additionally, in July 2016, the heads and presidents of the governments of the NATO Member States committed themselves to treating cyberspace in strategic

sense the same as the remaining three operational domains in their so-called "*cyber pledge*". Among other things, Member States pledged to:

- strengthen and enhance the cyber defences of national networks and infrastructures, as a matter of priority;
- allocate adequate resources nationally to strengthen their cyber defence capabilities;
- reinforce the interaction amongst their respective national cyber defence stakeholders to deepen co-operation and the exchange of best practices;
- enhance skills and awareness, among all defence stakeholders at national level, of fundamental cyber hygiene through to the most sophisticated and robust cyber defences;
- foster cyber education, training and exercising of their forces, and enhance their educational institutions, to build trust and knowledge across the Alliance.

The Government of Montenegro will continue to undertake activities towards the implementation of the strategic objectives defined in the Strategy so as to ensure further improvement of the concept of cyber security of Montenegro in order to be compatible with the concepts of the most developed EU and NATO Member States.

Special attention will be paid to harmonisation with regard to the standardisation of concepts, methods, policies and procedures in line with the accepted European and international standards.

1. Cyber defence capacities

According to the Global Cybersecurity Index¹⁰, drafted in 2017 by the International Telecommunication Union, Montenegro ranks 71st in the field of cyber security with a coefficient of 0.422,

¹⁰ Globalni sajber bezbjednosni indeks za 2017. Link: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf

out of 193 countries covered by this research. Compared to the region, Montenegro ranks higher than Albania (89), Serbia (90), Bosnia and Herzegovina (136), and Slovenia (84), while Croatia (41) and Macedonia (55) rank higher than Montenegro.

STRATEGIC OBJECTIVE:

The Government of Montenegro will continue its dedicated work on the further strengthening of the cyber security capacities in the sense of providing adequate human and financial resources as well as meeting other needs necessary for efficient and agile cyber capacities of Montenegrin institutions aimed at ensuring safe cyber space, providing business incentives and ultimately contributing to the economic prosperity of Montenegro.

PLAN OF ACTION AND INDICATORS:

a) Relevant institutions in the field of cyber security will establish CIRTs or identify staff members whose basic tasks will be related to the activities from the cyber security domain – so-called **local CIRTs**.

Indicator of success: the percentage-wise increase of the current number of CIRTs compared to the number of established teams and the number of institutions that should have CIRTs.

b) Relevant institutions must have capacities to recognise, identify and conduct annual risk analysis, or if necessary, risk analysis for a shorter period of time, which will be related to information systems within their own institutions or within their scope of work.

Indicator of success: the number of conducted risk analyses compared to the number of institutions.

c) Budgetary funds must be allocated every year to separate bodies or organisational units within institutions that have been identified as key for Montenegrin cyber security system so that they can procure adequate resources and tools for the effective functioning.

Indicator of success: the number of institutions which have budgetary funds intended for cyber security and the number of institutions that have a trend of increasing the annual budget for these needs.

d) Relevant bodies must define an optimal number of staff members in their CIRT, i.e. the number of employees who will be in charge of cyber security, with the aim of providing an adequate response to threats, challenges, risk analysis and possible attacks to their information systems. The previously said must be done at the annual level in order to obtain the current number of employees and also the necessary number of employees at the national level. ENISA¹¹ recommends that CIRT should have a minimum of 12 staff members for a fully staffed 24/7 shift.

Indicator of success: a report on the minimal number of staff members in charge of cyber security.

2. Centralisation of cyber expertise and resources

STRATEGIC OBJECTIVE:

The Government of Montenegro will undertake activities with a view to centralising and gathering expertise in the field of cyber security in order to: strengthen capacities for the purpose of responding efficiently to sophisticated cyber threats against critical information structures and other important information systems; understand risks to cyberspace of Montenegro;

¹¹ More information via link: <https://www.enisa.europa.eu/publications/csirt-setting-up-guide>

provide adequate recommendations and improve cooperation with the private and public sectors.

With regard to cyber capacities and defence, the leading states have started establishing cyber security and incident response independent institutions, which has proven to be a necessary and very efficient step. Thus, the United Kingdom of Great Britain and Northern Ireland established the National Cyber Security Centre (NCSC) in 2015, gathering several institutions, including the national Computer Incident Response Team (CIRT). In 2012, the Republic of Croatia established the Information Systems Security Bureau (ISSB) which also serves the function of a National CIRT, while Australia, apart from the Cyber Security Centre, representing a major cyber security capability, has also the Joint Cyber Security Centre, which brings together business, government and academia, and represents innovative and efficient approach to cyber security in the sense of better sharing of information and trust among different actors, strengthening of cooperation and pooling forces, in order to provide a unique response to cyber threats, attacks and challenges.

PLAN OF ACTION AND INDICATORS:

a) In line with the Strategy for the Development

of Information Society 2020, the National CIRT will have ten staff members by 2018, and 20 staff members by 2020.

Indicator of success: the fulfilment of set deadlines and the number of employees in the National CIRT.

b) National CIRT will have two departments - for incident response, of technical character, and for strategic goals, politics and preventive.

Indicator of success: amendments to the Rulebook on the Internal Organisation and Systematisation of working positions of the Ministry of Public Administration.

c) Two specialised rooms will be provided for operations of the National CIRT, where experts from other institutions will be allowed to work in the event of attacks against CII and large scale attacks against Montenegro.

Indicator of success: the number of rooms meeting a minimum of technical standards compared to the number of envisaged ones.

d) National CIRT will regularly organise specialist exercises, simulation of attacks against CII and large scale attacks, for members of relevant bodies, as well as companies accountable for CII.

Indicator of success: the number of organised exercises and actors included.

3. Protection of critical information infrastructure

No.	Critical sector	Accountable institution for critical sector
1.	Information and communication technologies	Ministry of Public Administration
2.	Banking and finance	Ministry of Finance
3.	Energy	Ministry of Economy
4.	Health care	Ministry of Health
5.	Agriculture, food safety, forestry and water management	Ministry of Agriculture and Rural Development
6.	National defence and security	Ministry of Defence Ministry of Interior Ministry of Justice National Security Agency
7.	Transport	Ministry of Transport and Maritime Affairs
8.	State authorities Services of the Government of MNE	Ministry of Public Administration

In accordance with the Cyber Security Strategy for Montenegro 2018-2021, the amendments to the Law on Information Security were adopted (Official Gazette of Montenegro, No 40/2016), through which formally and legally critical information structure have been defined as (previously it was defined through Methodology for selecting CII): „information systems of bodies which, if compromised or destroyed, would endanger the life, health, and safety of citizens, as well as the functioning of the country, while the performance of public interest activities depends on their proper functioning”.

A detailed analysis of information systems of the responsible authorities was drafted within the first stage.

A detailed analysis of information systems of the state authorities was drafted within the second stage.

Within the third stage, a questionnaire was sent to the private sector, on the basis of which the analysis of their information systems was acquired, thereby analyses of information systems of all critical sectors have been completed.

On the basis of the said analysis, and the analysis of criticality, a proposal list of critical information systems was adopted, after which the Government of Montenegro tasked the Ministry of Public Administration to adopt a final list of CII, and subsequently the define protection measures.

The European Union identifies two main methods for protecting CII: The first one, where the overall process is governed by the state, applied by Montenegro, and the second one, where the main function belongs to operators/owners of CII.

Eight critical sectors have been identified in Montenegro which include one or more CIIs: Security control of CII within a sector belongs to line ministries or other state authorities that have the legal basis and obligation for securing and regulating these sectors. National CIRT is a central

point for coordination of activities, development of cooperation and other activities related to this field.

Case study

In February 2017, a number of services belonging to the state authorities were under intensive and continuous DDoS attack, lasting for two weeks.

The analysis showed that the attack originated from a wide range of IP addresses spread all over the world, and represented a network of so-called zombies - compromised computers characteristic of this kind of attacks, and during this period of time, several state services were under a continuous cyber attack.

The said incident influenced on raising awareness of the consequences that can be caused by an attack in cyberspace. Simultaneously, the state authorities dealing with the defence had an opportunity to test their capacities and to develop faster and more efficient cooperation with partners from private sector with the aim of more efficient defence from this type of attacks.

STRATEGIC OBJECTIVE:

The Government of Montenegro will continue to strengthen the CII defence capabilities, and since the National CIRT has a key role in this field - it must have adequate resources and tools to effectively understand, analyse and respond to the wide spectrum of threats in this field.

The resources of state authorities in charge of safety control of CII must be adequate to the task, i.e. the state authorities must have staff members who understand threats and risks for specific CII belonging to their sector. Human and technical resources must be strengthened with the aim of efficient performance of this function.

With the aim of efficient defence, it is necessary to identify and essentially understand risks related to CII, namely related to the fields of action, different information platforms, systems, functions and technologies that CII is made up from, which is a complex task and a challenge. Bearing in mind that a large part of CII belongs to a private sector, the Government of Montenegro will provide support in identifying risks for critical systems, and, when necessary, establish additional protection measures aimed at protecting national resources.

The Government of Montenegro will also continue to improve the legislative framework, standards and obligations that the owners of CII must comply with, due to harmonisation with the EU Network Information Security Directive of European Parliament and of the Council.

PLAN OF ACTION AND INDICATORS:

a) Owners of identified CII are required to conduct annual risk analysis. National CIRT, in cooperation with other responsible CIRTs, is in charge of reviewing the analyses, and providing assistance in making analyses where CII owners do not have sufficient capacities.

Indicator of success: the number of conducted analyses compared to the number of CII, as well as their quality.

b) Adoption of secondary legislation for protecting CII. This regulation should define the procedures for communication between owners of CII and responsible institutions, as well as basic technical and organisational measures that owners of CII have to implement.

Indicator of success: an adopted Decree on measures for protecting CII.

c) National CIRT, in cooperation with other CIRTs, should establish and formalise strategic partnerships with owners of CII, where, among other

things, exchange of information should be specified, as well as the manners of exchanging information and expertise.

Indicator of success: the number of formalised partnerships with holders of CII.

4. Inter-institutional cooperation

STRATEGIC OBJECTIVE:

The need for strengthening inter-institutional cooperation has been identified, whereby a special accent will be placed on efficient and timely exchange of information and best practices. In this context, the responsible institutions will work on strengthening communication methods through, among other things, organisation of exercises for crisis communication in the case of cyber incidents and large scale attacks. The exercises will be aimed at defining clear communication procedures in crisis situations as well as their timely revision.

PLAN OF ACTION AND INDICATORS:

a) In order to further facilitate cooperation and communication among institutions, there is a need for appointing contact persons for cyber security on behalf of all actors involved.

Indicator of success: the number of appointed contact persons compared to the number of institutions.

b) Establishment of a publicly available registry of cyber experts which would be managed by the ministry responsible for this field.

Indicator of success: the functioning of registries of cyber experts.

c) Development of a platform for dialogue and exchange of information which would connect

cyber security experts from public and private sectors, both at local and national level.

Indicator of success: an operational platform.

d) Setting up of an inter-ministerial working group at technical level which would gather cyber security experts and create capacity to defend against cyber attacks.

Indicator of success: the formed inter-ministerial working group.

e) Inter-ministerial working group will organise simulations and exercises aimed at efficiency, coordination and communication.

Indicator of success: the number of organised exercises at annual level, duration of exercises as well as the number of covered situations.

f) Drafting of a rulebook and procedures for exchange of information on cyber incidents, the manner of communication in the event of cyber attacks, and the manner of assistance and co-operation among state authorities.

Indicator of success: a defined rulebook and procedures on the exchange of information on cyber incidents and communication among bodies.

5. Data protection

STRATEGIC OBJECTIVE:

For the purpose of providing an adequate protection of the important part of information infrastructure, the Government of Montenegro will strengthen the national capacities necessary for security accreditation of communication and information systems and the processes where classified information is used, as well as the capacities in the field of crypto protection.

The Law on Data Confidentiality acknowledges the principle of marking information with a certain level of classification and the way of dealing with these data, from those marked with the lowest level of classification whose disclosure would make harmful consequences for functioning of the body, to those with the highest level of classification whose disclosure would endanger or cause irreparable harmful consequences for security and interests of Montenegro. As a result of computerisation of business processes, these data are created, processed and kept electronically, and due to the need for efficient exchange of information, they are all the more transferred through cyberspace. With a view to providing adequate protection and raising the level of culture of handling classified and sensitive information electronically, it is necessary to strengthen the national capacities needed for the implementation of the legally prescribed security accreditation of communication and information systems and processes where classified data are marked as CONFIDENTIAL and SECRET, and also provide a proper management system for security of information in the systems where data marked as INTERNAL are used¹², as well as in the systems where unclassified sensitive data are handled. Also, it is necessary to plan national capacities in the long run with the aim of developing domestic cryptographic solutions.

PLAN OF ACTION AND INDICATORS:

a) In March 2017, a set of legal regulations was adopted necessary for implementing certification of communication and information systems and processes where secret data of higher classification are used. It has been recognised that there is a room for improvement of this set of regulations, particularly in the part of certification of "standalone" machines and inter-connection

¹² Law on Data Confidentiality (Official Gazette of Montenegro, No 14/13 of 15 March 2013) and the Decree on detailed conditions and manner of implementing measures of classified information protection (Official Gazette of Montenegro, No 57/10 of 1 October 2010)

of communication and information systems.

Indicator of success: the drafting of relevant legal acts and supporting documents by the inter-ministerial working group.

b) Strengthening of information capacities of the state authority in charge of security accreditation of communication and information systems and processes where classified information is used (Security Accreditation Authority - SAA), and the state authority responsible for handling materials for cryptographic protection of secret data (National Distribution Authority - NDA).

Indicator of success: the number of newly employed IT specialists in the Directorate for Protection of Confidential Data which will deal with accreditation of communication and information systems and with management of crypto materials.

c) Strengthening of the institutional capacities necessary for carrying out certification of communication and information systems and their inter-connections through the introduction of a systematised function that includes a job description for information security of classified information in state institutions where classified information is mostly handled electronically (for higher levels of classification a separate working position is provided, while for the lowest level of classification it is possible to add a job description to the existing working position).

Indicator of success: the number of systemised working positions with a job description related to information security of classified data.

d) Certification of communication and information systems where information marked with higher level of classification is used, the introduction of security information management system and risk management in communication and information systems where classified data marked as INTERNAL are used (ISO/IEC 27000 certification with additional security measures) and unclassi-

fied sensitive information (ISO/IEC 27001).

Indicator of success: the number of certified communication and information systems and the number of conducted internal reviews aimed at controlling the implementation of standards.

e) Establishing cooperation with educational and scientific institutions with the aim of long-term education and training of personnel, for the needs of creating national cryptographic solutions.

Indicator of success: the degree of established cooperation and the number of educational or scientific projects resulting from that.

6. Cyber security education

STRATEGIC OBJECTIVE:

In order to achieve the best cyber security practice, the responsible bodies will learn about the newest cyber threats and undertake activities on educating citizens and organisations about protection mechanisms in cyberspace. Sustainable, continuous and coordinated efforts are necessary to achieve wider changes in behaviour and secure that all target groups, public and private sectors, as well as individual citizens, understand risks and threats in cyberspace.

Raising awareness of threats in cyberspace and their influence on the overall society is of vital importance. Through raising awareness, individual and corporate users may learn how to behave and feel secure and ready to do business online.

Education of employees and citizens through publishing of various security tips, instructions and warnings is based on current trends in technology and distribution of relevant knowledge of regional and international experts. An important

segment in spreading awareness is also improving contents on the portal with materials, which are continuously updated in accordance with new technologies related to information security (guidelines, rulebook, presentations, webinars, lectures).

Focus on different target groups is a result of successful and efficient campaigns of raising awareness of security challenges. Continuous following and evaluation of campaigns serve for identifying new emerging needs and for adapting the campaign processes. Sustainable human and financial resources and continuous monitoring can contribute to increasing flexibility and adaptability of the campaigns.

PLAN OF ACTION AND INDICATORS:

a) In order to promote and spread the cyber security culture, it is necessary to progressively continue with participation in and organisation of conferences, workshops, trainings, as well as with production of publications, drafting of papers and articles, and participation in educational programmes.

Indicator of success: the number of held conferences/workshops/trainings and the number of appearing in educational programmes.

b. Given that constant education, following of trends and awareness raising are of major importance for cyber security, it is necessary to constantly improve the contents on the portal CIRT.ME, with materials related to security, which are continuously updated in accordance with the new technologies (tips, warnings, announcements, guidelines, rulebooks, presentations, webinars, lectures).

Indicator of success: an amount of published contents on the portal CIRT.ME and an amount of updated materials.

c) It is necessary to educate teaching staff in or-

der to raise their awareness of cyber security because they spend the most of the time directly working with children, so they are able to influence on raising awareness of this topic among children.

Indicator of success: the number of teachers trained according to the previously established training programme.

d) A special target group that has been recognised are school pedagogues and psychologists. The majority of problems in school are resolved in pedagogical and psychological service, therefore their knowledge and understanding of this topic is of great importance for helping children. Previously, it is necessary to determine whether all school pedagogues are digitally literate, and if not, it is necessary to teach them basic computer skills, and afterwards, carry out trainings related to cyber security.

Indicator of success: the number of trained pedagogues and psychologists according to the previously established training agenda.

e) Regular subject Informatics with Technique which is learnt from the fifth grade of primary school, comprising a certain number of lessons, is not sufficient when it comes to the topic of cyber security, therefore it is necessary to organise extra-curriculum activities for school-age children on these topics, especially for children of very young age.

Indicator of success: the number of held workshops, competitions, debates, and so on, as well as the number of children included in these activities.

f) It is necessary to develop a set of materials on various topics of cyber security which will be adjusted to various ages of children. Materials should be published on the school portal (www.skolskiportal.edu.me) in the category Online Security of Children.

Indicator of success: the number of created

materials (photos, videos, rulebooks, guidelines, recommendations, games, etc.).

7. Partnership of public and private sectors

STRATEGIC OBJECTIVE:

In the upcoming period, the Government of Montenegro will continue its dedicated work aimed at supporting the both - response to incidents and sharing of information and joint initiatives in partnership with private sector. Therefore, only high level of communication, cooperation and integration can be an efficient way to understand and properly respond to the needs and challenges of private companies, with the aim of undertaking the necessary measures and achieving a sufficient degree of security.

Improving of cyber security demands a combined, multi-user, comprehensive approach focused on cooperation with private companies. The cooperation provides, through joint research and exchange of experiences and practice, that no part of the critical infrastructure, whether in public or private hands, become a weak link and vulnerability.

Partnership of public and private sectors is an efficient tool in protecting national interests. Sharing of information, expertise and knowledge is a form of strategic partnership between shareholders from public and private sectors. In accordance with the Law on Amendments to the Law on Information Security, the Information Security Council has been formed, representing a framework for constant exchange of information among public administration, representatives of

the economy, science and research. The Information Security Council should provide procedures for exchanging information between state authorities and key private sector institutions, particularly the Internet provider, the banking sector and the Electric Power Industry of Montenegro (EPCG). Building of a successful public and private sectors partnership takes into consideration different elements as well as challenges and barriers that such structures can face. Establishing of efficient cooperation among stakeholders is one of the main challenges due to different interests, trust, competition and lack of clear managerial structure.

Companies reluctantly report security incidents due to potential loss of reputation, so building of trust is a process that requires an extensive dialogue, time and effort. Partnerships demand a clear framework which determines roles of public and private sectors, their relations and areas of cooperation.

PLAN OF ACTION AND INDICATORS:

a) With the aim of developing efficient response to cyber security, it is necessary to work on improving and institutionalisation of cooperation among public and private sectors.

Indicator of success: the number of established public and private partnerships.

b) Drafting of procedures for exchange of information on cyber incidents, the ways of communicating in the case of cyber attacks, the ways of assistance and cooperation between public and private sectors.

Indicator of success: a defined rulebook on procedure for exchange of information on cyber incidents and communication between public and private sectors.

8. Regional and international cooperation

STRATEGIC OBJECTIVE:

The Government of Montenegro will continue with its regional and international activities and exercise its influence by investing in partnerships which shape global evolution of cyberspace in the manner which improves and spreads economic and security interests and strengthens collective security.

Considering the global nature of the Internet and, consequently, the problems of cyber security, regional and international cooperation is necessary for securing the cyberspace of Montenegro.

Due to an increasing number of security incidents, the existing capabilities of Computer Incident Response Team (CIRT) are no longer sufficient. In order to provide a proper response and protect national interests, cooperation and activities with regional and international partners should continue.

It is necessary to further strengthen relations with bilateral and multilateral partners, including the EU, NATO, OSCE and UN, particularly through collective defence and collective security.

Such cooperation facilitates positive exchange of

experiences, knowledge and best practices, all of which contribute to the strengthening of national security. Therefore, Montenegro will continue to promote the participation of its representatives in international organisations, as well as in professional exercises and associations in this field.

PLAN OF ACTION AND INDICATORS:

a) As the exchange of regional and international experiences and best practices contributes to the strengthening and development of cyber security, the active participation should continue through joint exercises, trainings, meetings, fora, conferences, seminars.

Indicator of success: the number of held trainings, conferences, seminars, exercises, meetings, and it will be of qualitative character.

b) With a view to strengthening cooperation with key international institutions in the field of cyber security, it is necessary to continue cooperating with organisations that we belong to (FIRST, ITU, NATO), and work on establishing and promoting new partnerships.

Indicator of success: the number of established partnerships, signed agreements and memoranda.





06

Monitoring

For the purpose of providing an adequate implementation of the Cyber Security Strategy for Montenegro 2018-2021 and accompanying action plans, pursuant to Art. 13 para.1 of the Law on Information Security (Official Gazette of MNE, No 14/10 and 40/16), the Government of Montenegro adopted a Decision on forming the Information Security Council with the task, among others, to monitor the implementation of the Strategy and the action plans.

The bodies identified as accountable for activities defined by the Strategy and accompanying action plans are obliged to submit quarterly reports on the implementation thereof to the Information Security Council.

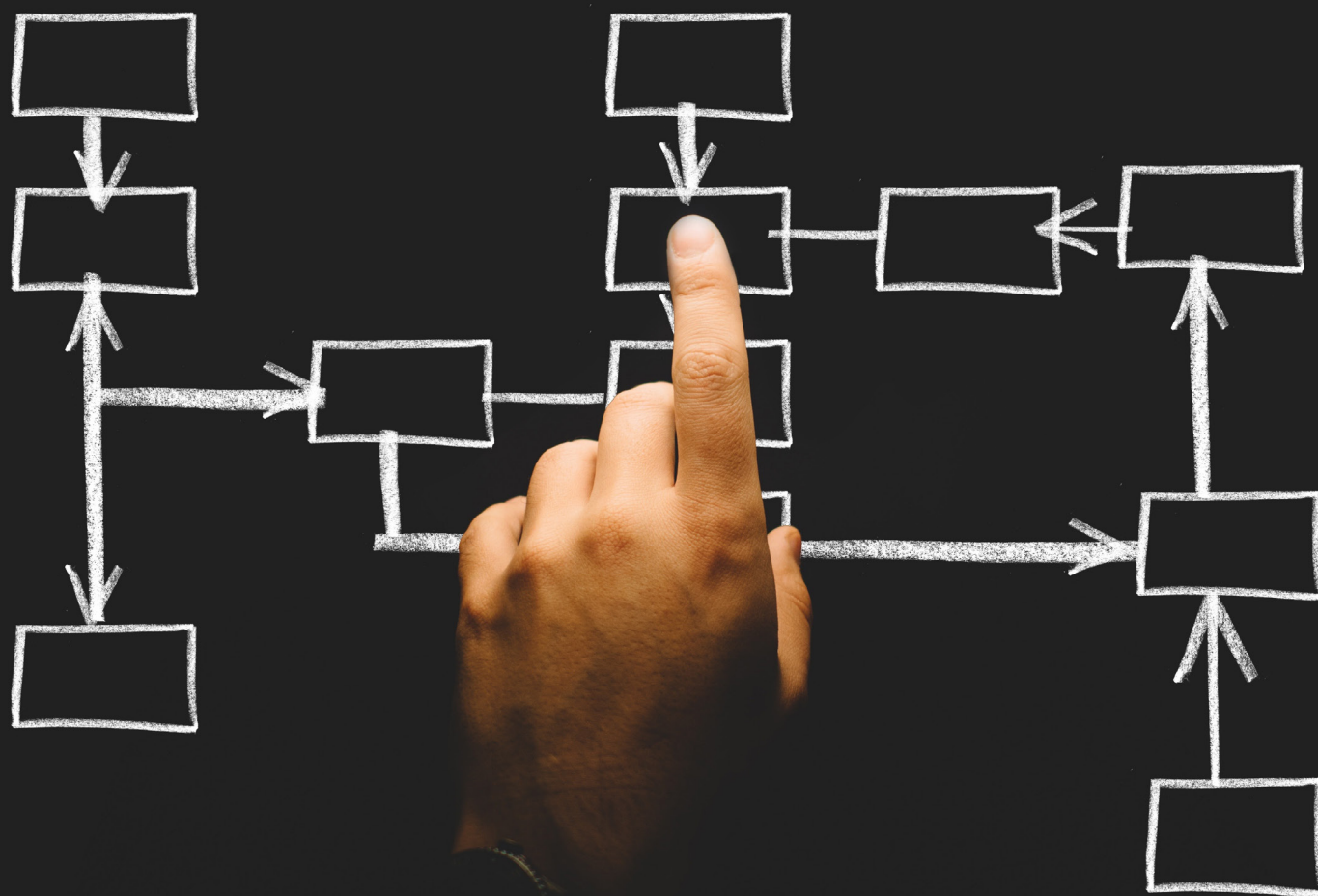
On the basis of the delivered reports, the Council will analyse the achieved results and, in accordance with its powers, give opinions and recommendations if the degree of the implementation does not follow the established dynamics.

The Council will submit annual performance reports to the Government, which will address the degree of fulfilment of strategic goals defined by the Strategy and activities from the Action Plan, and it will also contain proposal measures for further improvement of Montenegro's cyber security.



07

Concluding review



Security of Montenegrin cyberspace is of major importance for the overall security of the state and its citizens. Greater engagement of the representatives from the public, private, academic and civil sector in the upcoming period will contribute to providing cyber security.

Functioning of every individual in the modern era cannot be imagined without the use of information and communication technologies. Development of technologies stimulates the economic and social development of a state, ensuring its competitiveness and positioning in the region and Europe. Therefore, Montenegro cannot and must not be an exception.

Taking into consideration the previously said, and the fact that a number of threats in cyberspace is constantly growing, simultaneously with further development of information society, it is necessary to constantly work on improving cyber security.

The Government of Montenegro is devoted to growth and prosperity through strong cyber security.

In the past period, on the basis of Art. 13a of the Law on Information Security (Official Gazette of MNE, No 14/10 and 40/16), the Government of Montenegro adopted the Decision on forming the Council on Information Security. The Council will, inter alia, monitor the implementation of the Cyber Security Strategy, by delivering quarterly reports submitted by the bodies identified as the main holders of activities defined by the Strategy the accompanying action plans. In this manner, analyses will be conducted, and opinions and recommendations will be provided, in accordance with respective responsibilities of bodies, while

annually a performance report will be delivered to the Government of Montenegro.

When it comes to critical information structure of Montenegro, on the basis of the Cyber Security Strategy 2013-2017, amendments to the Law on Information Security (Official Gazette of MNE, No 40/16) were adopted, where critical information structure has been defined, and on the basis of that - eight critical sectors identified. The process of protecting CII is governed by the state of Montenegro, and this model of governance is one of the two management models in the European Union. National CIRT is a central point for coordination of activities, development of cooperation and other activities related to this field.

In the period to come, the Government of Montenegro will continue to strengthen cyber defence of CII, by providing adequate resources and tools for understanding, analysing and responding to threats by national CIRT and other state authorities in charge of controlling the security of CII.

This Strategy identifies a total of eight objectives for improving the National Cyber Strategy for Montenegro 2018-2021, namely:

1. reliance on European and Euro-Atlantic concepts,
2. strengthening the cyber defence capacities,
3. centralisation of cyber expertise and resources,

4. strengthening of inter-institutional cooperation,
5. data protection,
6. cyber security education,
7. strengthening partnership between public and private sectors,
8. strengthening regional and international cooperation.

Through clearly defined strategic aims, Montenegro will develop fully compatible concept with concepts of the most developed EU and NATO member states. Such concept will create a pre-condition for a more secure information society and provide successful implementation of the Cyber Security Strategy and existing legal regulations dealing with this field.

With the aim of strengthening cyber security capacities, the Government of Montenegro will continue to pay a great attention to providing additional human and financial resources and other needs of institutions which work actively on security of Montenegro's cyberspace.

Activities aimed at attracting a wider pool of cyber expertise and resources will ensure strengthening of capacities for responding to threats against critical information infrastructure and other systems of state importance, understanding of risks for Montenegro's cyberspace, provision of adequate recommendations and encouragement of cooperation between public and private sectors.

Also, Montenegro will strengthen national capacities necessary for security accreditation of communications and information systems and processes where classified information is used, as well as the capacities in the field of cryptographic protection of data.

The responsible institutions will actively work on strengthening inter-institutional cooperation, through efficient and timely exchange of information and best practices, organisation of exer-

cises and simulation of large scale attacks. In this way, clear procedures for communication in crisis situations will be defined and the shortcomings identified, to be eliminated in a timely manner.

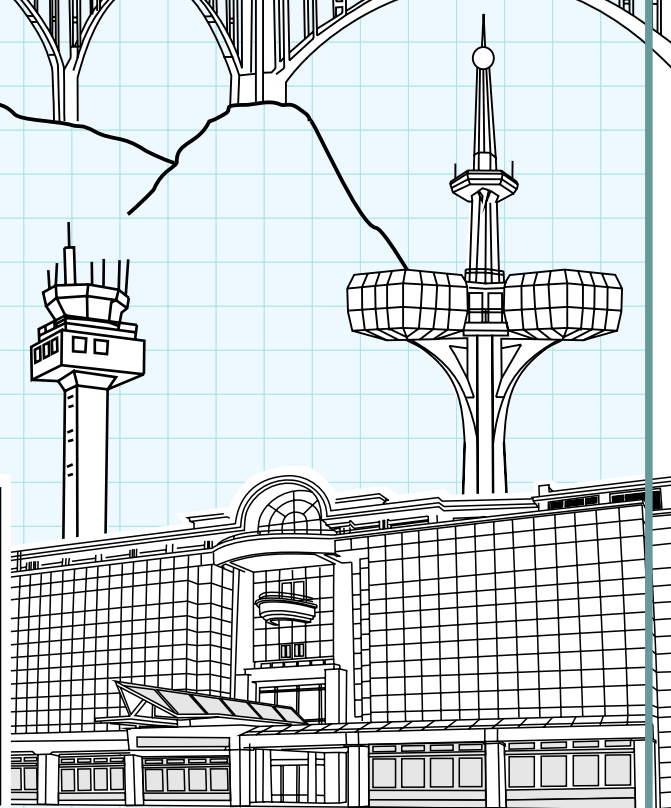
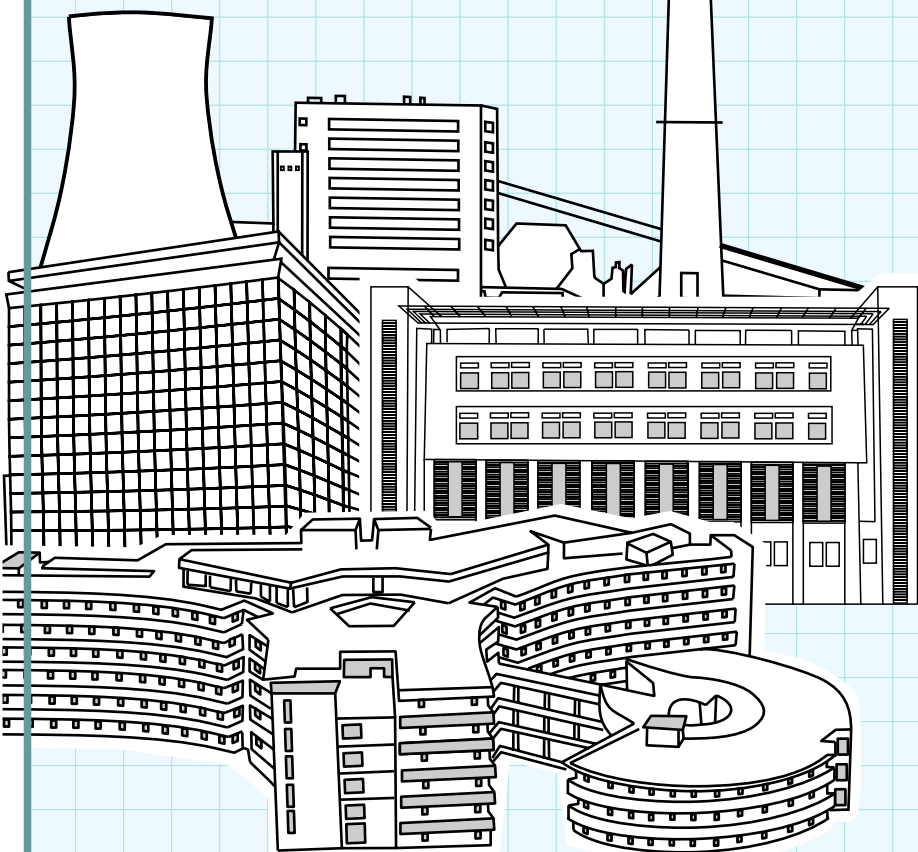
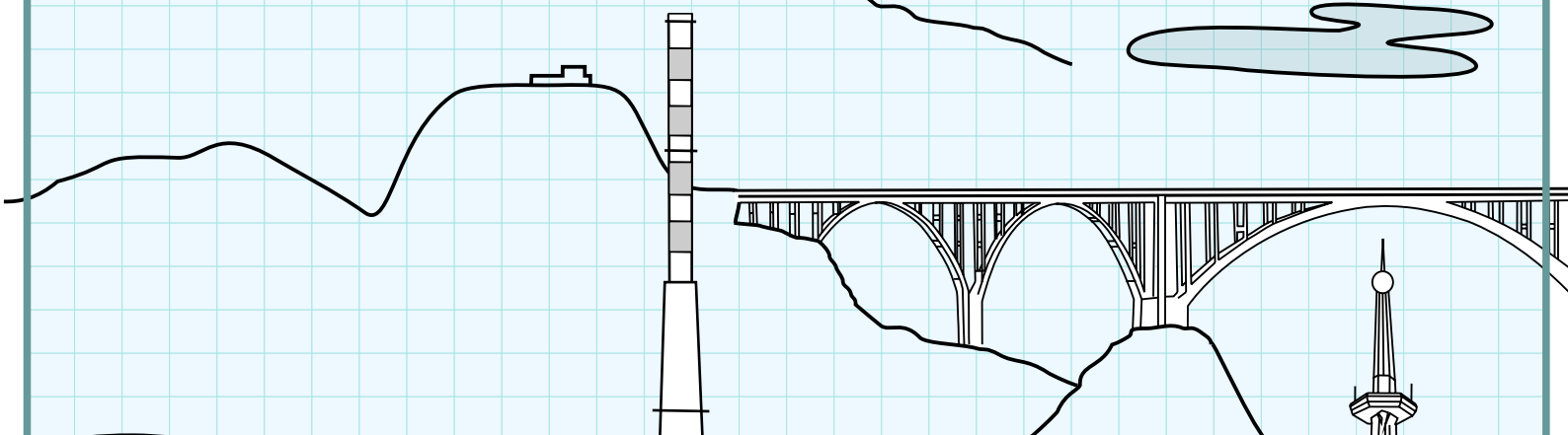
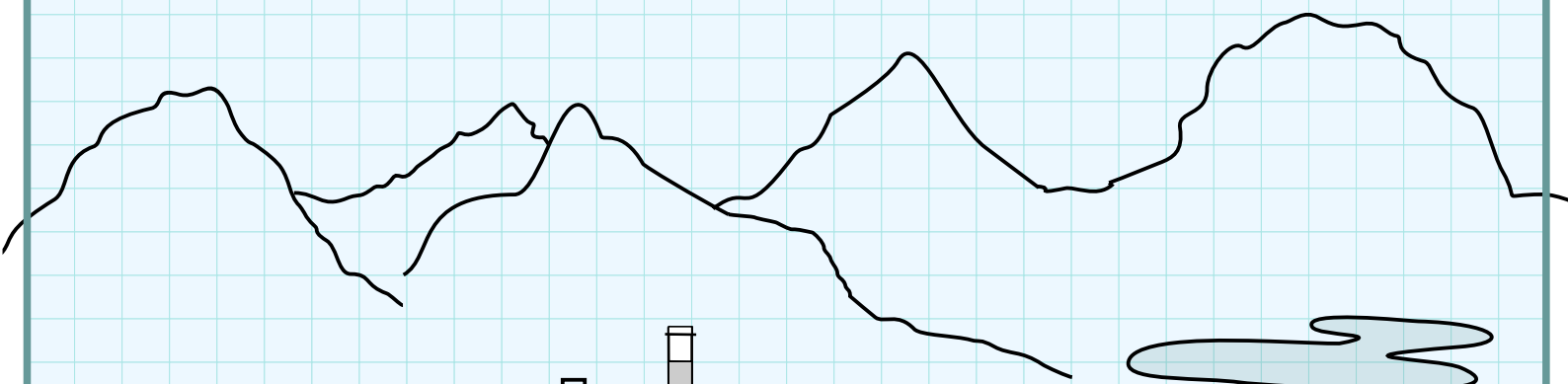
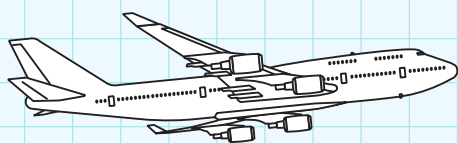
Regional and international cooperation is an important segment in providing national cyber security, so Montenegro will continue with regional and international activities and invest in partnerships, with the aim of improving and spreading economic and security interests, as well as improving collective security.

The Government of Montenegro will undertake further steps with the aim of raising awareness of the problem of cyber security of both - institutions and organisations, and citizens as well. Raising awareness through providing information on what should be done to protect oneself on the Internet will result in the overall change of behaviour and ensure that everybody is aware of protection at home, in school and at work.

In the period to come, the work on strengthening public and private partnerships will be continued with the intention of information sharing, launching of joint initiatives and response to incidents. Public-private partnership is the efficient way to understand and properly respond to the needs and challenges of private companies, with the aim of undertaking the necessary measures and achieving a sufficient degree of security.

Finally, safe cyberspace encourages favourable environment for further development and progress, to the satisfaction of all citizens.





CRITICAL SECTORS IN MONTENEGRO

The background image is a perspective view of a long, narrow corridor. The walls and floor are made of dark, vertically-oriented wooden planks. The corridor leads to a bright, rectangular opening at the far end, which appears to be a doorway or a window looking out into a bright, overexposed area. The lighting is dramatic, with the bright light at the end creating a strong contrast with the dark interior.

Annex

Definitions and terms

Active Cyber Defence

The principle of implementing security measures to strengthen the security of a network or system to make it more robust against attack.

Authentication

The process of verifying the identity, or other attributes of a user, process or device.

Autonomous System

A collection of IP networks for which the routing is under the control of a specific entity or domain.

Bitcoin

A digital currency and payment system.

CII

Critical Information Infrastructure

Cryptography

The science or study of analysing and deciphering codes and ciphers; cryptanalysis.

Cyber crime

Cyber-dependent crime (crimes that can only be committed through the use of ICT devices, where the devices are both the tool for committing the crime and the target of the crime); or cyber-enabled crime (crimes that may be committed without ICT devices, like financial fraud, but are changed significantly by use of ICT in terms of scale and reach).

Cyber incident

An occurrence that actually or potentially poses a threat to a computer, internet-connected device, or network – or data processed, stored, or transmitted on those systems – which may

require a response action to mitigate the consequences.

Cyber resilience

The overall ability of systems and organisations to withstand cyber events and, where harm is caused, recover from them.

Cyber security

The protection of internetconnected systems (to include hardware, software and associated infrastructure), the data on them, and the services they provide, from unauthorised access, harm or misuse. This includes harm caused intentionally by the operator of the system, or accidentally, as a result of failing to follow security procedures or being manipulated into doing so.

Cyberspace

The interdependent network of information technology infrastructures that includes the Internet, telecommunications networks, computer systems, internetconnected devices and embedded processors and controllers. It may also refer to the virtual world or domain as an experienced phenomenon, or abstract concept.

Cyber threat

Anything capable of compromising the security of, or causing harm to, information systems and internetconnected devices (to include hardware, software and associated infrastructure), the data on them and the services they provide, primarily by cyber means.

Cyber-physical system

Systems with integrated computational and physical components (so-called “smart” systems).

Data breach

The unauthorised movement or disclosure of information on a network to a party who is not authorised to have access to, or see, the information.

Domain

A domain name locates an organisation or other entity on the Internet with unique name registered in authorised institutions, so-called domain registries.

Domain Name System (DNS)

A system of mapping numeric IP addresses on domain.

E-commerce

Electronic commerce. Trade conducted, or facilitated by, the Internet.

Encryption

Cryptographic transformation of data (called "plaintext") into a form (called "cipher text") that conceals the data's original meaning, to prevent it from being known or used.

Incident management

The management and coordination of activities to investigate, and remediate, an actual or potential occurrence of an adverse cyber event that may compromise or cause harm to a system or network.

Incident response

The activities that address the short-term, direct effects of an incident, and may also support short-term recovery.

Industrial Control System (ICS)

An information system used to control industrial processes, such as manufacturing, product handling, production and distribution, or to control infrastructure assets.

Insider

Someone who has trusted access to the data and information systems of an organisation and can pose cyber threat.

Integrity of information

The property that information has not been changed accidentally, or deliberately, and is accurate and complete.

Internet

A global computer network, providing a variety of information and communication facilities, consisting of interconnected networks using standardised communication protocols.

Internet of Things

The totality of devices (vehicles, buildings, television sets, cameras...) and other items embedded with electronics, software and sensors that communicate and exchange data over the Internet and have IP address.

Malware

Malicious software, or code. Malware includes viruses, worms, Trojans and spyware.

Network (computer)

A collection of host computers, together with the sub-network or inter-network, through which they can exchange data.

Patching

Patching is the process of updating software to fix bugs and vulnerabilities.

Penetration testing

Activities designed to test the resilience of a network or facility against hacking, which are authorised or sponsored by the organisation being tested.

Ransomware

Malicious software that denies the user access to their files by encrypting them. A ransom is paid for the return of files.

Reconnaissance

The phase of an attack where an attacker gathers information on, and maps networks, as well as probing them for exploitable vulnerabilities in order to hack them.

Risk

The potential that a given cyber threat will exploit the vulnerabilities of an information system and cause harm.

Router

Devices that interconnect logical networks by forwarding information to other networks based upon IP addresses.

SMS spoofing

A technique which masks the origin of an SMS text message by replacing the originating mobile number (Sender ID) with alphanumeric text. It

may be used legitimately by a sender to replace their mobile number with their own name, or company name, for instance. Or it may be used illegitimately, for example, to fraudulently impersonate another person.

Social engineering

The methods attackers use to deceive and manipulate victims into performing an action or divulging confidential information. Typically, such actions include opening a malicious webpage, or running an unwanted file attachment.

User

A person, organisation entity, or automated process, that accesses a system, whether authorised to, or not.

Virus

Viruses are malicious computer programs that can spread to other files.

Vulnerability

Bugs in software programs that have the potential to be exploited by attackers.



GOVERNMENT OF MONTENEGRO
MINISTRY OF PUBLIC ADMINISTRATION