6TH INTERNATIONAL STUDENT CONFERENCE ON LOCAL SAFETY AND SECURITY

UNIVERZITET CRNE GORE
PRAVNI FAKULTET

University of Maribor
Faculty of
Criminal Justice and Security

arrs
SLOVENIAN RESEARCH AGENCY

COMPUTER CRIME PREVENTION IN MONTENEGRO

Ina Ivanović
Tijana Krivokapić
Jelena Medojević
Ljubica Samardžić

Content

Introduction ⇒ basic terms

- *Technology development*- improving communication and ways of doing business
- *Range of abuse* - it is classified as a subtype of the economic crime
- *High-tech crime* - quick and easy profit for both individuals and organized criminal groups
- *Internet crime* - Commiting of criminal offenses that have Internet as a Global Computer Network as their subject and object, and that are committed by IT skilled individuals with the aim of causing harmful consequences or obtaining illegal property benefits
- Basic *characteristics* of Cyber crime

What is the Cyber Crime?

Two main types of cyber crime:

- The crime enabled by cyber tools, which refers to "traditional" forms of crime that are now being transferred to cyberspace, such as economic crimes, crimes against the safety of children and young adults, and even acts of terrorism

- Advanced cyber crime (also known as high-tech crime), which refers to sophisticated attacks targeting computer hardware and software

The main targets?

- Individuals
- Companies
- Public institutions
- Non-profit organisations

Classification of cyber crime

According to the recommendation of the Council of Europe on computer crime No. R(89)9, later specified in the Convention on Computer Crime, the following are listed as criminal acts:

1) Computer fraud
2) Computer forgery
3) Computer sabotage
4) Unauthorized access
5) Unauthorized reproduction of a protected computer program
6) Unauthorized reproduction of protected topography
7) Changing computer data or programs
8) Computer espionage
9) Unauthorized computer use
10) Unauthorized use of protected computer programs and topographies

Hacktivism

By definition, it is a combination of hacking and traditional activism.

Ordinary hacktivism generally causes less harm, which is why very few cases result in prosecution.

Hacktivism is considered disruptive, not destructive. This distinguishes it from other forms of malicious activity in cyberspace, such as cybercrime and cyberterrorism.

Hacktivism is the misuse of a computer or the internet to expose a believed injustice.

Politically motivated

hacktivism seeks to promote or upheave a political agenda, sometimes to the extent of anarchy.

Socially motivated

hacktivism sets out to shed light on social injustices, spanning from government censorship to human rights.

Religiously motivated

hacktivism acts in the name of a religious ideology, whether that's to discredit or encourage the belief.

White, Grey and Black Hat hackers

Because hacktivists are essentially hackers with a purpose, different types of hackers are distinguished based on the specific activities they undertake when they enter a system. They can be:

- White hat hackers reveal weak points of the system that they report to the system designers, in order to develop specific patches and improve the overall security of the system. White hat hackers are also described as "ethical hackers".

- **Gray hat hackers also report discovered vulnerabilities to system designers, but they may seek compensation or some other type of reward for the information they provide.**

- **Black hat hackers do not report discovered vulnerabilities to system designers and instead they seek to profit by either directly exploiting or selling that information on the black market to other parties, such as cybercriminals.**

Cyber espionage

It is defined as an action undertaken in secret or under false pretenses using cyber facilities to collect (or attempt to collect) information with the intention of transmitting it to an opposing party.

Cyber espionage is normatively considered both acceptable and unacceptable, depending on the consequences.

There is a fine line between actions whose primary objective is cyber espionage and actions that are considered outright cyber attacks.

From a security perspective, cyber espionage is considered to potentially overlap with ideas of cyber crime.

Attack cycle

- Phase before the attack
- Phase during the attack
- Phase after the attack

Strategy on cyber crime of Montenegro

Cyber Security Strategy of Montenegro 2022-2026. is an interdepartment document that refers to a five-year strategic period and is aimed at improving overall capacities (legislative, operational, human, financial and technical) for an adequate response to challenges and threats that come from cyberspace in/and outside of Montenegro.

During the preparation of the Draft Strategy, *the strategic framework of the European Union*, which deals with the issue of cyber security, was considered, so that when formulating strategic goals and further activities, they would be in line with the long-term directions of development in this area.

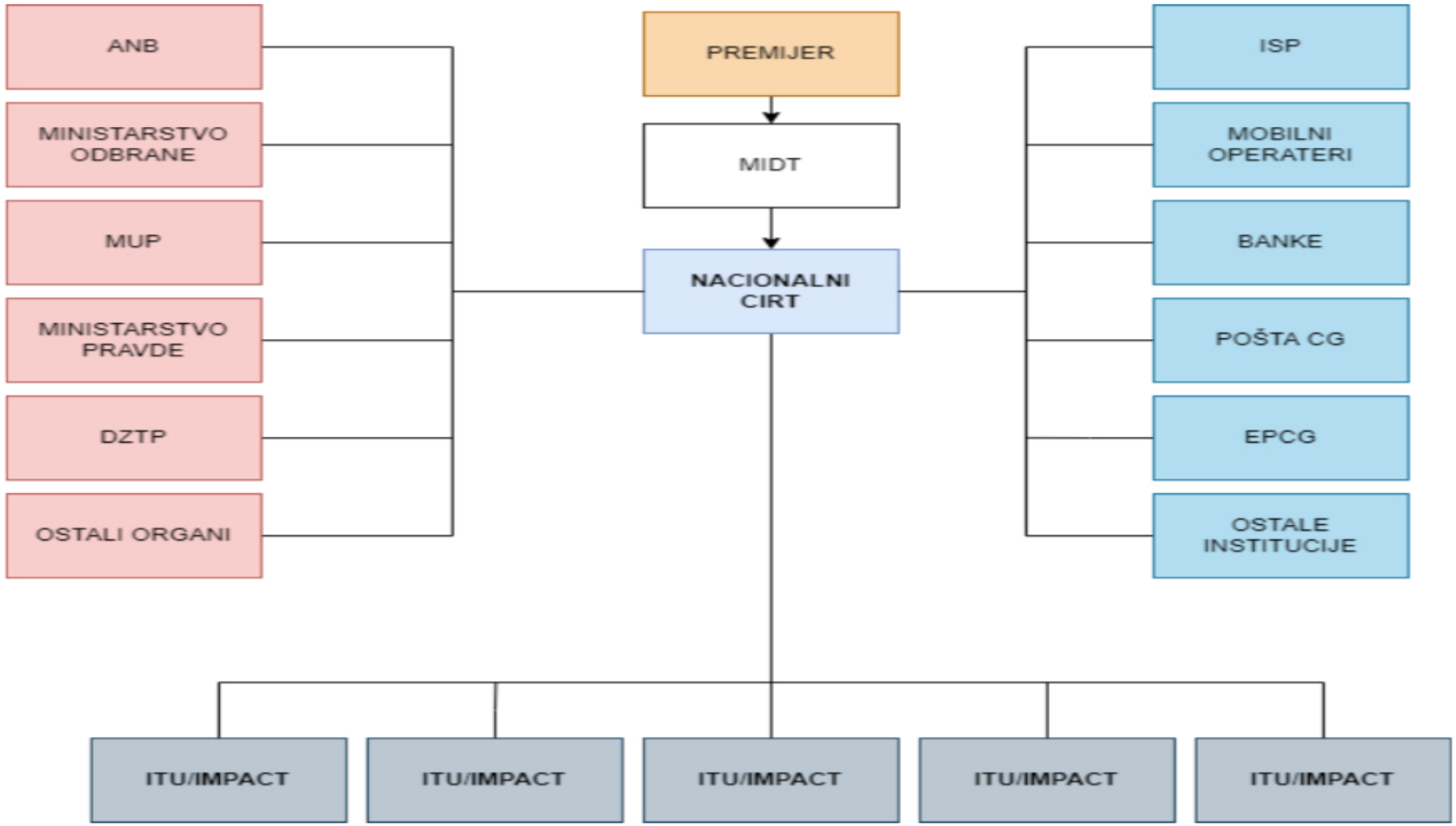
The principle of compliance and the principle of transparency were respected during the drafting of the Strategy.

Security system holders in Montenegro

In Montenegro, the following institutions are recognized as key in the field of cyber security:

- Ministry of Information Society and Telecommunications (National CIRT)
- Ministry of Defense
- Ministry of Interior affairs
- Ministry of Justice
- National Security Agency
- Police Directorate
- Army of Montenegro
- Directorate for the Protection of Secret Data
- Universities of Montenegro

Prikaz pozicija Nacionalnog CIRT-a u sistemu sajber bezbjednosti u Crnoj Gori



Cyber crime in Montenegro

In 2022, the first major attack on the Government of Montenegro took place. Political scandals have been happening in Montenegro for a number of years, and the hacker attack on state institutions further worsened the state of institutions, which led to the inability to use basic systems (the website of the Government of Montenegro, Health, Tax Administration, etc.).

Attacks on the information network of the Government of Montenegro began on August 22, when access to their websites and emails, as well as those of other institutions such as prosecutor's offices, courts, was disabled...

At the beginning of September, FBI experts arrived in Montenegro to help overcome the consequences of cyber attacks on state institutions.

The Ministry of Defense on September 12. announced that the USA will donate 23 million dollars to equip the Montenegrin Army, and that a special focus will be on strengthening cyber defense capacities, in light of new attacks.

Also, in addition to hacker attacks, there were numerous reports of bombs planted in state institutions, shopping centers, and to this day it is not known who reported it.

Conclusion

Computer crime entails enormous economic and financial losses, both for the individuals and for society as a whole, violates privacy, causes material and non-material damage through a specific method of operation as well as means of committing criminal acts.

In order to suppress this global problem and to reduce the existing crime rate, it is necessary to:
reform the existing legislation, form special investigation teams, make an adequate strategy to fight against it, establish international cooperation, work on preventive measures and tighten criminal sanctions.

Montenegro needs the training of officials who are in charge of maintaining the IT system of the country.

Literature

- Directive of the Council of Ministers of the European Union 2013/40/EU.
- Council of Europe High-tech Crime Convention (CETS 185).
- Lutovac, S., Račić J., (2021): Computer crime as a modern form of crime, Belgrade.
- Stamenković B., Balota A., (2014): High-tech crime, a practical guide through contemporary criminal law and examples from practice, Podgorica.
- Cyber Security Strategy 2022-2026, Podgorica.