https://doi.org/10.55843/SG2321085p

NORMATIVE FRAMEWORK TOWARD CYBERCRIMES IN NORTH MACEDONIA

Assist. Prof. Dr. Vesna Poposka[1]

ABSTRACT

Cyber security is relatively new area, which covers all aspects of modern living.Specific nature of cyberspace, its specific structure and immateriality, makes it complex to provide. Nonetheless the original intention of cyberspace was not to be "secured" or even less, controlled. Things have changed and today it is sensitive and critical area, and the Achilles heel of modern society. One of

The main challenge from normative perspective is to make effective criminal law and enable application. The aim of the paper is to provide a comprehensive approach to the issue and provide with the key legal infrastructure over the area in North Macedonia, in order to further find recommendations and realistic guidelines for effective threat management, proportionately to the needs and demands of democratic societies.

The subject of the paper is a global issue in local context, and the main goal is to extract the existing legal norms that are relevant, since North Macedonia does not have a specific law on cybersecurity, although recently National cyber security strategy was adopted.

Keywords: cybercrimes, law enforcement, penal code

Assist. Prof. Dr. Vesna Poposka

Faculty of Law, International Vision University, Gostivar N.Macedonia

e-mail: vesna.poposka @vizyon.edu.mk

UDK: 343.9:004(497.7)

Declaration of interest: The authors reported no conflict of interest related to this article.

INTRODUCTION

Although it is universally agreed that cybercrime exists, there is no universal definition of what it means (Holt and Bossler, 2014; Wall, 2017a).

The (mis)use of cyberspace and the benefits of modern technology allow a large reach and quick benefit to achieve various political goals. Non-state actors take advantage of modern technology to multiply power every day.

Often, the states themselves, acting openly or covertly, abuse the same space, entering into proxy wars, using all elements of national power to gain a certain advantage or to achieve a goal that supports their national interest.

Technological development is no longer a luxury, it is a necessity. It defines and improves the quality of life of individuals and societies and this conclusion got completely different dimension in the pandemic world, since the biggest part of all of the activities and communications is moved online. On the other hand, that is what makes our society and each individual more vulnerable in every way possible - our public privacy is a compromise between the need for security and the realization of the liberal concept of individuality and human rights.(Nuredin, 2022) Internet access is slowly but surely becoming part of the complex of recognized human rights.

Whereas traditional crimes are decreasing in Western countries, cybercrimes are increasing beyond this rate of reduction (Caneppele and

Aebi, 2019). It has also been noted that decreases in traditional crime predate the emergence and growth of cybercrime (Farrell et al., 2015).

THE COMPLEXITY OF CYBER CONTEXT

The complexity of cyberspace and the security threats that arise from it, causes real effects in all aspects of everyday life. The question often arises as to whether cyberspace can be a "crime scene" or just a tool to commit it. Unfortunately, both options are possible. The enormously rapid technological advances that have made life easier and accelerated economic processes and globalization have made the world we live in more vulnerable. From a security point of view, cyberspace is the new "Achilles' heel" - or rather, hic sunt leones ("here lions are hiding" - figuratively, a Latin proverb).

The complexity of cyber offences takes a great range of activities, such as:

a) cyber attack, a term that covers a wide range of activities with different character and purpose, even activities that could activate Article 5 of the Washington Treaty, ie provoke a military response in terms of collective self-defense of NATO member states;

b) cybercrime includes criminal activities carried out using computers and the Internet, usually financially motivated. Cybercrime includes identity theft and fraud, among other activities. Cybercrime differs from other forms of malicious cyber activities that have political, military or espionage motives;

c) cyber war or "Intentional use of computer systems in order to interrupt the activities of an enemy country, or attack its communication

systems. To determine a state of cyber warfare, there must be an attribution of actions to government agents or government agencies. The author is of the opinion that it is the proving of attribution that is often the main "culprit" that the world is not at least officially, even in cyber warfare;

d) cyber warfare is a hybrid term that aims to cover a wider range of aggressive actions. Unlike war or crime, the term "war" is not a legal category. That is why it is often used - it covers a wider range of actions, especially in the context of modern hybrid and asymmetric security threats, which are often found in the space between crime and war. The context in which it is most commonly used includes a state or an alliance of states as an entity and as at least one party.

e) Cyber terrorism - a term used to refer to acts of terrorism in cyberspace, but also the use of cyberspace as a tool for committing acts of terrorism. It can fall under any of the above categories depending on the specifics of the individual circumstances.(Schmitt, M. 2013).

In wider context, cyber security usually refers to safeguards and activities that can be used to protect the cyber domain, both in the civilian and military areas, from those points that are connected to, or through which independent networks may be harmed, information and their infrastructure.

CRIMINAL JURISDICTION IN CYBER DOMAIN

From data theft and financial embezzlement to disabling services, espionage, compromising critical infrastructure and direct attack on a nuclear program - the range is really wide. That is why it is very difficult

to give concrete and specific legal answers that would meet the requirements of different challenges. The very structure of cyberspace, and especially the nature of the Internet, is the opposite of the need to be controlled. The first key legal question would be: whose jurisdiction is it?

The territorial context of the law is primarily related to jurisdiction. For example, courts adjudicate on the basis of ratione loci (territorial jurisdiction) and ratione material (actual jurisdiction). In the context of critical infrastructure, this means that they will be responsible for civil or criminal proceedings related to critical infrastructure in a given territory. Sometimes, however, jurisdiction can be replaced by another instance - for example, arbitration, or through other mechanisms (Poposka, 2019).

Although the jurisdiction of the states is primarily territorial, in some cases it can be exercised outside the territory of the state. Given the subject matter and purpose of the International Covenant on Civil and Political Rights, it is natural for its provisions to apply in any case. The Court also refers to the practice of the Human Rights Committee, which is originally responsible for the interpretation of the ICCPR, which is consistent with this view - the Committee considered the Covenant to be applicable even when States exercise acts under their jurisdiction in foreign territory.

All universal agreements oblige countries to establish their extraterritorial jurisdiction over acts committed abroad in at least two cases: when the act was committed by one of their nationals (active personal principle) - the alleged perpetrator is on the territory of the state and has not been extradited to any state seeking extradition for the same conduct (the so-called "aut dedere aut judicare" principle).

In other cases, counter-terrorism conventions provide optional grounds for jurisdiction, e.g. in case of offenses committed abroad against (principle

of passive identification). Some acts are also prosecuted on the basis of the real protection principle: such is the crime of counterfeiting money, regardless of which country the currency belongs to. Criminal law theory also knows the principle of universal jurisdiction, but it is rarely applicable in practice.

From the practice of the states, three main trends for incrimination can be distinguished i) criminalization of behavior related to specific types of infrastructure (sectoral approach);

ii) criminalization of behavior against chritical infrastructure in general (cross-sectoral approach);

iii) rely on specific criminal legislation that does not directly address critical infrastructure (indirect approach). (UN,2018)

The incrimination is primarily intended to have a deterrent effect on potential future perpetrators, and which method of implementation is more appropriate depends on the relevant legal tradition. In any case, in order to enable international assistance in criminal matters, it is necessary that the offense be criminalized in the national law of the countries concerned. At the same time, the ability of individual countries to prosecute offenders effectively will often depend on the effectiveness of existing international channels of law enforcement cooperation, refugee surrender, and the exchange of evidence.

Of particular importance, in case when cyber offence is conducted, countries from a criminal point of view should consider the role of universal counter-terrorism instruments in providing a legal basis for extradition and mutual legal assistance, either in addition to or in the absence of bilateral or regional agreements on this effect.

Eventually we can talk about jurisdiction over the infrastructure that enables the existence of cyberspace, but in essence, it is not a fixed category. The world of bits and bytes cannot be measured, located and allocated in the classical sense of the term. Cyberspace, on the other hand, is a place where most spears are "broken" in a clash between security and privacy requirements, and human rights are conceptually under attack. In the absence of a consensual legal response, it remains to achieve maximum applicability of the existing legal regimes depending on the specific situation, ie to perform a separate analysis for individual cases. In addition to the different factual situations that require different applicable legal regimes, different approaches to cyber culture and cultural relativity as such should be taken into account, the dependence of a particular society on cyberspace, its resilience to threats, the intent of potential attackers, and the effects and consequences measured in the specific harm of a possible attack. The vocabulary used in this domain is also not unified, which leaves additional space for interpretation.

Material criminal law aspects

When it comes to the national legal framework, in the Republic of North Macedonia cyber security is treated primarily in the field of cybercrime, in a narrower sense, ie it comes down to the classic acts of cybercrime or the use of computer systems and networks to commit acts of "classical "Crime - (computer) fraud, (computer) forgery, theft (of personal data), etc., ie the national legal framework moves primarily through the substantive criminal law - the Criminal Code.(Кривичен законик на РСМ) The Criminal Code recognizes a few different criminal offences related to cyber:

- Article 144, paragraph 4 - Endangering security

"The one who will threaten to do it through an information system a criminal offense punishable by up to five years in prison or a more severe sentence against a person because of his or her affiliation with a particular national, ethnic or racial group or religion, shall be punishable by one to five years' imprisonment. "

- Article 147 - Violation of the secrecy of letters or others shipments
- Article 149 - Misuse of personal data (.... He who contrary to the conditions established by law without the consent of the citizen collects, processes or uses his personal data, will fines or imprisonment of up to one year. A penalty from paragraph 1 shall be imposed on anyone who enters a computer Information system of personal data intentionally using them for yourself or to reap some benefit or to inflict some benefit.) The attempt is also punishable.
- Article 149-a - Prevention of access to public information system
- Article 157 - Violation of copyright and related rights
- Article 157-a - Violation of the right of the distributor oftechnically specially shielded satellite signal
- Article 157-b - Piracy of an audiovisual work
- Article 157-c - Piracy on a phonogram
- Article 193 - Showing pornographic material on minor
- Article 193-Production and distribution of children pornography;
- Article 251 - Damage or unauthorized entry in a computer system
- Article 251- Making and importing computer viruses; Computer fraud;

- Article 271 - Making, procuring or alienating means of counterfeiting
- Article 274-b - Making and using a false payment card
- Article 279-a - Computer forgery
- Article 286 - Violation of the right from a reported or protected invention and topography of integrated circuits
- Article 394-d - Dissemination of racist and xenophobic material through a computer system

LAW ON CRIMINAL PROCEDURE AND OTHER INSTRUMENTS

In addition to the Criminal Code, the Law on Criminal Procedure (Закон за кривична постапка is also relevant, which refers to procedural norms in general, and which equally apply to the prosecution of cybercrime offenses criminalized by the Criminal Code. data (Article 184) and temporary seizure of computer data (Article 198), and partly in the part related to measures for finding and securing persons and objects, as well as in the part for special investigative measures (secret inspection and search in computer system and insight into realized telephone and other electronic communications).

The procedural aspect of cybercrime issues is refers to the measures and actions that apply specifically to this type of crime, as well as the measures and actions applied in conventional crime. Those are the provisions related to search of computer system and computer data (Article184) and temporary seizure of computer data (Article 198), as well as the provisions of Chapter XVII - Measures for finding and securing

persons and cases, further purpose and types of special investigative measures (Article 252) especially the special measures of secret inspection and search in a computer system and insight into realized telephone and other electronic communications, etc. Cybercrime, like conventional crime, presupposes gathering evidence that despite their physical presence requires and collecting data that is not visible15 and is in a form that presupposes their prior detection and fixation through the physical form (computer, workstation, telephone, etc.) and then download additional procedural actions that presuppose indirect contact with evidence in electronic form and places where it is stored. (Зврлевски, М, Андонова,С, Милошески В. 2014)

Additionally, certain segments are covered by:

• Law on Electronic Communications

• Law on Interception of Communications

• Law on Electronic Commerce

• Law on Electronic Government (e-government)

• Law on Data in Electronic and Electronic Forms signature.

The Republic of North Macedonia is a member of the Council of Europe Convention on Cybercrime (CoE,2001). With the ratification of the Convention, it becomes part of the internal legal process in accordance with the Constitution .

The Convention on Cybercrime is the first international agreement dealing with crimes committed through the Internet and other computer networks, dealing specifically with copyright infringement, computer fraud , child pornography and network security breaches

It also contains a series of authorizations and procedures, such as computer network search and interception. Its main goal, in the spirit of the preamble, is to pursue a common policy aimed at protecting society from cybercrime, in particular through the adoption of appropriate legislation and the promotion of international cooperation.

It contains material and procedural aspects, in order to harmonize the legislation between its member states.

The Convention is also the most important international legal act in the field. Although there are other regional initiatives and documents, it is considered the most specific and comprehensive so far. The initiatives go so far as to recently propose a draft document establishing an international cybercrime tribunal, but in principle quantitatively, the number of initiatives is far greater than the realized projects or concrete effects.

In principle, both the national legal framework and the Council of Europe Convention deal with cybercrime and basic offenses. In terms of cyber warfare and cyber warfare, an epic endeavor is the preparation of the Tallinn Manual on International Law Applicable to Cyber Warfare, prepared by a group of experts, with the intention of providing answers and codification.

North Macedonia became the 103rd member of the Global Forum on Cyber Expertise (GFCE) , one of the world's largest networks for international cooperation and capacity building for cyber security. Through GFCE, work will be done to increase the international cooperation and coordination of the Government and the organizations that provide support and work on the cyber theme in North Macedonia,

for which GFCE has developed a platform for monitoring and coordinating projects and activities. (META,2022)

CONCLUSION

When it comes to the national legal framework, in the Republic of North Macedonia, cyber security is treated as a criminal matter, primarily in the domain of cyber crime. That is, it comes down to the classic acts of computer crime or the use of computer systems and networks for committing acts of "classic" crime – (computer) fraud, (computer) forgery, theft (of personal data) and the like. The national legal framework moves primarily through substantive criminal law - the criminal code.

All things considered, 'on paper' the situation may not be so bad, but although there is no publicly available data or research on the extent of vulnerability, the certainty of risk is high.

The attack on the website of the State Election Commission is probably the most egregious example of this.

In recent months, North Macedonia and the countries of the region have been the target of intensified cyber attacks, which have been reflected in the hacking of websites of state institutions, intrusions into databases and the infection of systems with harmful software (malware). Although there is no single entity behind these attacks, their frequency can be linked to several common processes, such as exploiting the weakness of NATO member countries, but also diplomatic crises, such as the case between Albania and Iran (Faktor,2022).

Still, there was rarely anyone to bear criminal responsibility.

Additionally, the most serious problem is probably awareness, which needs to be intensively worked on, in parallel with the development of media literacy and the development of resistance, that is, resilience as a concept. In the absence of a precise legal framework and with a realistically hard-to-achieve consensus around it, the key actors in the world focus much more on the development of "policies" as a modus operandi for action and reaction.

The issue of dealing with cybercrime is complex as it often involves international borders and multiple legal jurisdictions. Different countries may have different laws regulating cybercrime, and the lack of cooperation or coordination between countries may hinder the investigation and prosecution of cybercrime.

Therefore, international cooperation and collaboration are crucial to effectively combat cybercrime. Countries must work together to establish common legal frameworks and cooperation mechanisms to investigate and prosecute cybercrimes and facilitate the exchange of information and expertise.

Moreover, countries must also ensure that their domestic laws and law enforcement agencies are equipped to handle cybercrime effectively. This includes strengthening cybersecurity measures, providing appropriate training and resources to law enforcement personnel, and promoting public awareness of cybercrime and its consequences. The issue of cybercrime poses a significant challenge to law enforcement agencies and requires a concerted and coordinated effort to address it effectively.

REFERENCES

1. Bossler AM, Holt TJ, Cross C, et al. (2019) Policing fraud in England and Wales: examining constables' and sergeants' online fraud preparedness. Security Journal 33: 1–18.
2. Caneppele S, Aebi MF (2019) Crime drop or police recording flop? On the relationship between the decrease of offline crime and the increase of online and hybrid crimes. Policing: A Journal of Policy and Practice 13(1): 66–79.
3. Council of Europe, Convention on Cybercrime, 23 November 2001, available at: https://www.refworld.org/docid/47fdfb202.html [accessed 20 June 2023]
4. Faktor (2022) Сајбер напади ја дрмаат Македонија и регионот available at https://faktor.mk/sajber-napadi-ja-drmaat-makedonija-i-regionot---koj-stoi-zad-niv
5. Farrell G, Laycock G, Tilley N (2015) Debuts and legacies: the crime drop and the role of adolescence-limited and persistent offending. Crime Science 4(1): 1–10.
6. Goldsmith A, Wall DS (2019) The seductions of cybercrime: adolescence and the thrills of digital transgression. European Journal of Criminology 19: 98–117.
7. META (2022) Северна Македонија стана членка на светската мрежа за сајбербезбедност,available at https://meta.mk/severna-makedonija-stana-chlenka-na-svetska-mrezha-za-sajber-bezbednost/
8. Nuredin A. (2022) Uluslararası İnsan Hakları Hukuku, Vision University Press.

9. Poposka, V. (2019) Меѓународно-правни аспекти за заштита на критичната инфраструктура од современи безбедносни закани, Изданија на Меѓународен Универзитет Визион-Гостивар
10. Schmitt, M. (2013). Short form citations. In Tallinn Manual on the International Law Applicable to Cyber Warfare (pp. Xiv-Xx). Cambridge: Cambridge University Press.
11. UN (2018) The protection of critical infrastructures against terrorist attacks: Compendium of good practices available at https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021/Jan/compendium_of_good_practices_eng.pdf
12. Закон за кривичната постапка (Службен весник на РМ, бр. 150 од 18.11.2010 година) со измените достапен на https://www.jorm.gov.mk/wp-content/uploads/2016/03/Zakon_za_Krivicna_postapka_150_18112010-2.pdf
13. Зврлевски, М, Андонова,С, Милошески В. (2014) - Прирачник за компјутерски криминал /OSCE
14. Кривичен законик, Пречистен текст (заклучно со „Службен весник на РМ“ бр.55 од 2013) со измените, достапен на https://jorm.gov.mk/krivichen-zakonik/