IRASA International Scientific Conference
SCIENCE, EDUCATION, TECHNOLOGY AND INNOVATION
SETI VI 2024
Book of Proceedings

DOI: `https://doi.org/10.62982/seti06.ankl.58

HIGH-TECH CRIME IN THE REPUBLIC OF SERBIA

Anita Klikovac[204], Sanela Veljković[205], Milica Ćurčić[206]

Abstract

High-tech crime encompasses a diverse set of illegal activities that take place in cyberspace. This new type of crime is becoming more and more prevalent with the development of information and communication technologies. Hacking attacks, identity theft, cyber espionage, various frauds and distribution of illegal content over the Internet represent different types of high-tech crime. In today's world, states must be able to adapt to the rapid and continuous development of technology in order to successfully suppress high-tech criminal activities. The fight against this phenomenon requires an adequate legal framework, various protection measures, as well as international cooperation. The reason for this should be found in the principle that high-tech crime does not stop at the borders of states. The paper aims to examine the very concept of high-tech crime, its various forms, as well as the most important normative provisions and institutional mechanisms that exist in the Republic of Serbia.

Key words: *High-tech crime, cyber crime, Republic of Serbia.*

Introduction

In today's digital age, high-tech crime represents one of the most significant challenges facing modern society. The development of information technologies and the increase in connectivity through the Internet have created new opportunities for various forms of criminal activity. High-tech crime encompasses a wide range of illegal activities that use or are linked to technological tools and infrastructure. This form of crime includes, but is not limited to, computer fraud, cyber attacks, identity theft, malware distribution, as well as various forms of digital espionage. Its complexity and dynamics often exceed traditional forms of criminal activity, which creates challenges for the justice system, police agencies and other institutions tasked with fighting

[204] Anita Klikovac, PhD Candidate, MSc student at Faculty of Security Studies, Belgrade, Republic of Serbia, anitaklikovac@yahoo.com
[205] Sanela Veljković, PhD Candidate, Junior Researcher, Vinca Institute of Nuclear Sciences – National Institute of the Republic of Serbia, Department of Physical Chemistry, Belgrade, Republic of Serbia, sanela.veljkovic@vin.bg.ac.rs.
[206] Milica Ćurčić, PhD, Research associate, Vinca Institute of Nuclear Sciences – National Institute of the Republic of Serbia, Department of Physical Chemistry, Belgrade, Republic of Serbia, milica.curcic@vin.bg.ac.rs

crime. High-tech crime is often intertwined with other types of crime, such as organized crime or terrorism, which further complicates its suppression and prosecution of the perpetrators. Certain aspects of high-tech crime form the core of the problems facing crime detection and prosecution institutions. First of all, it is a relatively new phenomenon, the specifics of which the competent authorities are not sufficiently familiar with. On the other hand, the methods and means used in the execution of criminal acts are constantly changing and improving with the development of information technologies, which inevitably leads to an increase in the gap between the knowledge of perpetrators and the (lack of) knowledge of authorized officials. For this reason, the specialization of competent authorities is necessary in order to adequately combat high-tech crime. It is important to point out that with the increasing influence of information technologies in the daily life of individuals and institutions, the complexity of high-tech crime is also increasing. This form of crime encompasses a wide range of activities ranging from unauthorized access to electronic systems, Internet fraud, to more serious threats such as cyber-attacks, the spread of malicious software and data theft.

The concept of high-tech crime

High-tech or computer crime, often defined as such in the literature, as well as in the general public, includes specific criminal activities characterized by the misuse of information technology, especially computers or networks. This type of crime refers to the commission of certain crimes through the practical operationalization of information technologies, including computers and networks. Given the intensive and dynamic development of computer technologies, it is extremely challenging to precisely define and determine high-tech crime. High-tech crime, according to the Law on the Organization and Jurisdiction of State Authorities for Combating High-Tech Crime, includes the commission of criminal offenses in which computers, computer systems, computer networks, computer data, as well as their products in material or electronic form, serve as an object or means of execution [1]. The concept of high-tech crime does not fundamentally differ radically from the concept of conventional crime. Both include conduct that involves the commission or omission of acts that lead to violations of the law and are subject to sanctions. In the context of high-tech crime, as with conventional crime, the behavior of individuals or organizations that can cause harm or violate law and order is analyzed. As a response to such behavior, sanctions, i.e. punishments, are prescribed in order to preserve legality and social order [2].

High-tech crime can be defined as criminal activity that includes information technology, infrastructure, unauthorized access, illegal interception through IT devices, damage, destruction, modification or suppression of data, and influence on the functioning of the information system through the entry, transfer, damage, destruction or deletion of data. This definition also includes aspects such as data theft, fraud and other similar activities [3]. In a phenomenological sense, the catalog of criminal activities that includes computer crime is growing more and more in

accordance with the development of information technologies. These activities can be classified into several categories: conventional crime that uses information technology and cyberspace for illegal activities; production and distribution of harmful software; cyber piracy; cyber fraud; cyber manipulation – stalking and indecent offers, usually of a sexual nature; cyber intrusions; cyber bullying; cyber terrorism, cyber warfare, cyber vandalism and cyber sabotage [4].

High-tech crime in the Republic of Serbia

Legal regulation of cyber space in the Republic of Serbia is not adequate and complete, and security challenges in the virtual world are constantly growing and transforming. The legal framework includes regulations regulating the authorities' competences for managing security risks in information and communication systems and suppressing actions that threaten or disrupt the functioning of these systems, as well as norms on techniques, methods and procedures for protection, coordination between protective factors, as well as norms on techniques , protection methods and procedures, as well as in terms of suppressing actions that threaten or disturb the functioning of these systems, their responsibility and supervision over the implementation of legal powers and obligations. In addition, the normative framework includes regulations that regulate protection against high-tech crime and other illegal threats in cyberspace, including preventive and repressive measures, as well as substantive and procedural norms, especially in the area of criminal legislation. This legal framework consists of the provisions of various laws, in which the security of information and communication systems is the primary or secondary subject of regulation [6].

Chapter twenty-seven of the Criminal Code of the Republic of Serbia regulates criminal offenses against the security of computer data. This category of criminal offenses includes: damage to computer data and programs (Article 298), computer sabotage (Article 299), creation and introduction of computer viruses (Article 300), computer fraud (Article 301), unauthorized access to protected computers, computer networks and electronic data processing (Article 302), preventing and limiting access to a public computer network (Article 303), unauthorized use of computers and computer networks (Article 304) and creating, obtaining and providing to others means for committing criminal acts against the security of computer data (Article 304a). Damage to computer data and programs, in the sense of the Criminal Code of the Republic of Serbia, means unauthorized deletion, damage, concealment or any other procedure that makes computer data or programs unusable. Computer sabotage is a criminal offense manifested by entering, destroying, changing, damaging, concealing or rendering unusable a computer or any other device for electronic processing and data transmission. The goal of computer sabotage is to disable and disrupt the process of electronic processing and data transmission of importance to state bodies, public services, institutions, companies and other subjects.

The Serbian legislator also sanctions the creation and introduction of computer viruses into someone else's computer or computer file. In the Criminal Code of the Republic of Serbia, the legislator included all forms of computer fraud, defined as entering

incorrect data, not entering correct data, concealing data or presenting it untruthfully. Unauthorized access to a computer and computer network or unauthorized access to electronic data processing are specially sanctioned. Also, the legislator sanctions unauthorized disabling or limiting access to public computer networks and unauthorized use of computers and computer programs. As a separate criminal offense in the Criminal Code of the Republic of Serbia, there is the criminal offense of creating, obtaining and giving to another person funds for the commission of criminal offenses against the security of computer data, which occurs in the case of production, sale, procurement for the purpose of use, importation, distribution of funds for the commission of a criminal offense against the security of computer programs [7].

Although classification is of great importance in the study of these works, we believe that it is not necessary to make artificial divisions in all ways. Regardless of the number of categories of high-tech crimes we identify, there will always be individuals who defy established logic and cannot be placed into pre-defined categories. From this, the following groups of high-tech crimes can be identified [8]: 1) crimes against computers and computer systems in the narrower sense; 2) criminal acts against copyright and related rights; 3) acts of a racist and xenophobic nature; 4) child pornography; 5) computer fraud; 6) other acts involving the use of computers and computer networks.

In the period from April 2005 to March 2009, the legislator of the Republic of Serbia enacted several key regulations for the implementation of the Council of Europe Convention on High-Tech Crime and the Additional Protocol into the national legal system. These regulations include the Law on the Organization and Competence of State Bodies for Suppression of High-Tech Crime, the Criminal Code, the Law on Liability of Legal Entities for Criminal Offenses, the Code of Criminal Procedure, the Law on Police, the Law on Copyright and Related Rights, the Law on Telecommunications, the Law on Electronic signature and the Law on Special Powers for the Effective Protection of Intellectual Property Rights. In March 2009, the National Assembly of the Republic of Serbia ratified the Convention on High-tech Crime and the Additional Protocol. After that, there were significant changes and other important regulations in this area. These steps created an institutional framework for a more effective fight against high-tech crime. Although the new legal solutions represented significant progress in the fight against high-tech crime, there were also some criticisms. The dark toll for this type of crime remains high, leading to questions about the effectiveness of the new legislation. Therefore, further research is needed to determine whether the changed legal framework and social environment in Serbia contributed to the improvement of the fight against high-tech crime [9].

In April 2005, the aforementioned Law on the Organization and Competence of State Authorities for the Fight against High-Tech Crime was adopted. In order to detect, process and try these criminal acts, it is necessary to form specialized units within the existing state bodies. The specialized police service for combating high-tech crime works to secure relevant evidence for computer crime and electronic piracy. This Service is part of the Criminal Police Directorate of the Ministry of Internal Affairs. Its managers are appointed and dismissed by the Minister of Internal Affairs with the

opinion of the special prosecutor. The Department for Combating High-Tech Crime cooperates with other organizational units, and in particular with the Department for Collection and Processing of Digital Evidence within the Service for Special Investigation Methods. It also cooperates with other organizational units of the Police Administration and certain security services of the Republic of Serbia, as well as with foreign services. In the last few years, the Department for Combating High-Tech Crime has established a wide range of cooperation, including cooperation with the National Central Bureau of Interpol Belgrade. This cooperation is particularly important due to the fact that high-tech crime often crosses borders and is a form of cross-border crime. Also, it is important to point out that the National Central Bureau of Interpol Belgrade is available 24 hours a day, seven days a week, which enables a quick exchange of information and effective action in the fight against crime.

Current trends

Publicly available data on cybercrime in the Republic of Serbia confirm the general trend of crime growth through the use of modern information technologies, which unequivocally indicates an increase in the risk to the security of citizens and institutions. One of the Internet security watchdogs reveals that 60% of respondents have experienced a computer virus infection at least once [10]. In addition, 14% of respondents stated that they had at least once experienced hacking of their personal account on one of the social networks. Also, a smaller number of respondents (8%) reported a case of fraud during an electronic purchase. In relation to the attacker, it is an interesting fact that almost half of the respondents (40.54%) consider themselves accidental victims, that is, they assume that they do not know the attacker (40.85%). On the other hand, a small number of respondents (3.93%) believe that the attack was the work of criminals who tried to steal data or money.

According to the research of the Register of National Internet Domains of Serbia (RNIDS) for the year 2022, the number of Internet users in Serbia reached about 74 percent, which is a significant increase in the last decade. This trend is accompanied by an increasing number of computer and mobile device users, which contributes to increasing connectivity via the Internet, but at the same time increases security risks. According to the RNIDS report, a significant number of Internet users have experienced cyber attacks, and a large part of them are not familiar with the identity of the attackers or are not even aware that they were the target of an attack [11]. In addition, most citizens are not sufficiently informed about the different types of high-tech crime. In Serbia, in the last three years, there has been an increase in the crime of endangering security, especially when threats are sent via social networks, which characterizes the elements of high-tech crime. Human rights defenders, environmental activists and journalists are particularly at risk. In the last three years, from January 2019 to June 2022, the SHARE Foundation registered 92 criminal charges related to endangering the safety of these groups of people. Attacks on these social groups have become frequent and almost routine, and the lack of sanctions only encourages this type of crime. The second most frequent criminal offense with

elements of high-tech crime in Serbia is the abuse of children for pornographic purposes via the Internet. The assessment of the threat of organized crime on the Internet for the year 2021, carried out by EUROPOL, indicates an increase in materials related to the exploitation of children for pornographic purposes on the Internet, which seriously burdens the capacities of the police and prosecutors around the world, including in Serbia [11].

Conclusion

Detecting high-tech crime is an extremely complex process that requires constant adaptation of legal, technological and intelligence capacities. In the context of rapid technological development, it is necessary to improve the cooperation of state authorities, the private sector and the academic community in order to jointly work on the prevention, detection and suppression of this form of crime. The effectiveness of court proceedings is based on the establishment of clear regulations, continuous education of lawyers and investigators, as well as investment in technological resources necessary for conducting investigations in a high-tech environment. It is also important to ensure that these efforts are consistent with the protection of civil liberties and rights, given the sensitivity of data and privacy in the digital space. From a legal perspective, detecting and proving high-tech crime is a challenge for justice systems around the world. Legal norms related to this area must be dynamic and adaptable to rapid changes in the technological environment. Lawmakers are faced with the need to define and update high-tech crimes to encompass new forms of cyber threats. The existence of precise and clear legal frameworks is essential to ensure successful prosecution. This paper points to the necessity of global coordination and international cooperation in dealing with cyber threats, given the transnational nature of high-tech crime. Through the constant improvement of legislation, technological capacities and intelligence methods, we can create a resilient and efficient system that will respond to digital security challenges in the future. The implementation of the Convention on High-tech Crime and its Additional Protocol into the national legal system of the Republic of Serbia represents a significant step towards a more effective fight against this form of crime. By adopting key regulations and harmonizing legislation with international standards, an institutional framework was created that enables more effective suppression of high-tech crime. Although the new legal solutions represented progress, there is a need for further research to assess the effectiveness of the new legislation and determine whether changes in the legal framework and social environment have contributed to the reduction of this type of crime. The key is the continuous improvement of cooperation between state authorities, the private sector and the academic community in order to adequately respond to the challenges of high-tech crime and preserve digital security.

Acknowledgements

This work was supported by the Ministry of Science, Technological Development and Innovation of Republic of Serbia; grant number 451-03-66/2024-03/200017

References

[1] Zakon o organizaciji i nadležnosti državnih organa za borbu protiv visoko tehnološkog kriminala, „Službeni Glasnik RS“, br. 61/2005, 104/2009, 10/2023, i 10/2023- dr.zak.
[2] Đukić Anđelija, Organizovani visokotehnološki kriminal- pojam, razvoj i osnovne karakteristike, *Vojno delo 70,* (2018), 3, 128-156. DOI: 0.5937/vojdelo1803128D.
[3] Degan, Vladimir Đuro, Pavišić Berislav i Beširević Violeta, *Međunarodno i transnacionalno krivično pravo,* Pravni fakultet Univerziteta Union, Službeni glasnik, Beograd, Srbija, 2011.
[4] Prlja Dragan, Korać Vanja i Diligenski Andrej, Maloletnici i sajber criminal, u *Maloletnici kao počinioci i žrtve krivičnih dela i prekršaja*, (Ivana Stevanović ur.) Beograd: Institut za kriminološka i sociološka istraživanja, Beograd, Srbija, 2015, 349-364.
[6] Milošević Mladen i Putnik Nenad, *Sajber bezbednost i zaštita od visokotehnološkog kriminala u Republici Srbiji - strateški i pravni okvir, monografska studija*, Fakultet Bezbednosti, Beograd, Srbija, 2017.
[7] Krivični zakonik, („Službeni glasnik RS“, br. 85/2005, 88/2005- ispr, 107/2005-ispr, 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016 i 35/2019)
[8] Reljanović Mario, Visokotehnološki kriminal: pojam, regulativa, iskustva, *Strani pravni život, 3,* 2007, 75-98.
[9] Milošević Mladen i Nikač Željko, *Izmene u zakonodavstvu Republike Srbije i borba protiv visokotehnološkog kriminala*, Univerzitet Singidunum, Beograd, Srbija, 2019.
[10] Bezbednost korisnika interneta u Srbiji, Registar nacionalnog internet domena Srbije (RNIDS), Beograd, 2022.
[11] Pavlović Marija, *Borba protiv visokotehnološkog kriminala u Srbiji, dostignuća i izazovi*, Beogradski centar za bezbednosnu politiku, Beograd, Srbija, 2022.