Acta Universitatis Danubius
JURIDICA

Cyber Security and Impact on Computer Crimes

Andrei Pântea[1]

Abstract: In the era of information technologies, it is demonstrated that cyber security and computer crimes are two interdependent elements that influence each other inversely proportionally in the conditions where the first one advances, the second one decreases, and vice versa. Many times, the persons responsible do not draw due attention to the need to strengthen cyber security, and law enforcement bodies, through the lens of the existing criminal framework, can hardly cope with cyber-attacks, information warfare, the massive influence on electoral processes, the manipulation of public opinion, from platforms and well-organized fake profiles and run from specific interest groups and command centers, equipped with the latest computer technologies and trained specialists. These would be just a few dangers that threaten the democratic processes in society, including the security of the state with the risk of deviating from the path proposed for the Republic of Moldova - the path to the European Union.

Keywords: cyber security; information warfare; cyber-crime; cyber terrorism; cyber espionage

1. Introduction

The impact of the process of digitization and technological advancement can be considered the primary factor contributing to the essential changes in society and the way in which complex operations are managed, which influence the development of contemporary society. Cybersecurity, as a mechanism, represents a set of people, processes and practical techniques that have the primary purpose of protecting critical infrastructures, digital businesses and sensitive information,

[1] Associate Professor, PhD, University of European Studies of Moldova, Republic of Moldova, Address: Strada Ghenadie Iablocikin 2/1, Chișinău 2069, Republic of Moldova, Corresponding author: andreipantea.posta@gmail.com.

exposed to internal or external threats, or even to negligence in management. The reality would be that social entities do not keep up with the latest digital trends, moreover, neither even the national nor the community legislation manages to fully regulate the current digital mechanisms, or to keep up with the common security level of the new forms of confrontations: cyber-crime, cyber terrorism, cyber espionage or cyber warfare.

The essence of cyber security, however, remains the protection of IT qualities and mechanisms that have become a necessary resource for society, namely: confidentiality, integrity and accessibility.

2. Results and Discussion

The biggest debate on this issue is a fundamental question about the trust and security of the Internet, or even the entire technology industry.

The Internet as a mechanism was never programmed with a built-in security system, and today it is well known that the digital environment can be easily compromised and exposed to cyber-attacks. For decades, the security industry was viewed with skepticism by cybercriminals. Attackers were mostly opportunistic, preying on weakly protected users who did not resist. And if they encountered well-secured systems, the attackers were not interested. Today, cybercriminals are actually highly motivated experts, mostly by criminal organizations or nation-states (Miller, 2014, p. 13).

As threats become increasingly sophisticated, the principle of security must evolve from fear of attack and risk to institutional and legislative harmony, to an understanding that establishing and maintaining trust and security can and will be a differentiating factor. Across industry and across governments.

At the current stage, the reality is that cyber-attacks are becoming more and more sophisticated. Attackers have a set of strategic advantages over those who have the mission to protect the system, namely: the advantage of taking the target by surprise, the ability to research and document on the victim of the cyber-attack, but also the complexity of the entire infrastructure and uneven regulations in the matter of cyber security and combating computer crimes.

The Government of the Republic of Moldova approved the National Cyber Security Program of the Republic of Moldova for the years 2016-2020, where it defines cyber security as: a state of normality resulting from the application of a

complex set of proactive and reactive measures that ensure confidentiality in cyber space, the integrity, availability, authenticity and non-repudiation of information in electronic format, information systems and resources, public and private services. Proactive and reactive measures include security policies, concepts, standards and guidelines, risk management, training and awareness activities, implementation of technical solutions to protect cyber infrastructures, identity management, and consequence management[1].

Also, the Information Security Concept of the Republic of Moldova was developed and approved by Law no. 299 of 21.12.2017. In accordance with art. 3 of the Concept of Information Security, SIS developed and jointly finalized with the competent national authorities the draft of the Information Security Strategy of the Republic of Moldova for the years 2019-2024 and the Action Plan for its implementation, approved by Parliament Decision no. 257 of 22.11.2018.

The accelerated development of modern information and communication technologies raises to another level the approach to threats, risks and vulnerabilities in an information society. Today, worldwide, cyber-attacks are increasing in frequency, complexity and scale, causing enormous damage to the government, private sector and citizens due to their asymmetric nature. Unauthorized access to electronic communications networks and services, unauthorized modification, deletion or damage of computer data, illegal restriction of access to this data and cyber espionage constitute constraints at the global level. Threats and risks, cyber-attacks and incidents, as well as other events occurring in cyberspace materialize through the exploitation of human, technical and procedural vulnerabilities. The economic damages resulting from the exploitation of such vulnerabilities are quite significant.

To date, no cyber security audit has been carried out, there are no studies or reports that would reflect in detail the situation regarding cybercrime in the Republic of Moldova, cyber threats and risks, cyber-attacks and incidents, other events occurring in cyber space, the number victims and the economic damages of their materialization.

The major danger of these events occurring in cyber space, where there are no borders, required that the agenda of a number of countries, starting from 2009,

[1] Government Decision no. 811 of 29.10.2015, regarding the National Cyber Security Program of the Republic of Moldova for the years 2016-2020 [On-line]: http://lex.justice.md/viewdoc.php?action=view&view=doc&id= 361818&lang=1.

include the issue of cyber security as a dominant topic. Already 56 states in the world have approved policy[1] documents in the field of cyber security, including 21 states of the European Union.

The internal legal framework of these countries conforms accordingly to the provisions of the Council of Europe Convention on computer crime, adopted in Budapest on November 23, 2001, taking into account the Recommendations of the International Telecommunication Union regarding cyber security.

The Republic of Moldova ratified the Council of Europe Convention on computer crime through Law No. 6-XVI of February 2, 2009. At the same time, Law no. 20-XVI of February 3, 2009 on the prevention and combating of computer crime was adopted, amendments and additions were made to the Criminal Code in accordance with the provisions of the ratified Convention, but its procedural provisions, as well as those related to the development of the 24/7 network contact point have not yet been implemented.

Based on the analysis carried out, the basic problem was identified - the lack of a cyber-security management system, within which to coordinate the planning and use of available resources, the identification of vulnerabilities and risks following the cyber security audit, the necessary interventions to reduce the impact harmful effect of cyber-crime, attacks and incidents on the secure development of the information society. This system is to be extended in all spheres of social, economic and political life. It must be created and implemented by the concerned public and private entities.

The lack of a cyber-security management system of the Republic of Moldova also generates the lack of complete, true, updated and structured statistical data, which, in turn, imposes some limitations in the analysis performed and the identification of optimal solutions. The effectiveness of the measures taken to develop a secure information society in the Republic of Moldova, technological and scientific advancement, the active participation of citizens in social and cultural life, as well as the country's economic growth dynamics depends on the result of solving the basic problem.

The national legislative-normative framework is not fully harmonized with the provisions of the Council of Europe Convention on cybercrime, the concerned institutions do not have clear powers regarding ensuring cyber security.

[1] https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-csss/national-cyber-security-strategies-in-the-world.

In order to regulate the examination process of an IT system or an IT data storage medium and to exclude a series of legislative barriers in the process of ensuring information security by the competent bodies, Law no. 294 of 22.12.2016 regarding the amendment and completion of art. 118 of the Criminal Procedure Code of the Republic of Moldova no. 122-XV of 14.03.2003.

The project in question, developed by the MAI, was to amend and complete the Law on the prevention and combating of computer crime, the Law on electronic communications, the Contravention Code, the Law on the exercise of the medical profession, the Criminal Code, the Code of Criminal Procedure, the Law on to international legal assistance in criminal matters. The project in question was developed according to the provisions of the Budapest Convention, the Lanzarote Convention, the EU directives and the legislative practice of the EU member countries, approved positively by the Venice Commission with the subsequent inclusion of improvement proposals in terms of guaranteeing the rights of individuals.

At the same time, the MIA mentions that, in order to regulate the examination process of an IT system or an IT data storage medium, Law no. 294 of 22.12.2016 for the completion of article 118 of the Criminal Procedure Code of the Republic of Moldova no. 122-XV of March 14, 2003. On 02/03/2017 this Law was published in the Official Gazette no. 30-39, art. 67.

Also, the General Police Inspectorate of the MIA submitted for approval to the Prosecutor's Office for Combating Organized Crime and Special Cases proposals to amend the Criminal Code and the criminal procedure code in terms of computer crimes.

Following a study of the situation in the field of preventing and combating computer crimes, they submitted proposals to adjust the national legislation to the international one, which aim to:

- adapting the provisions of the Criminal Code in order to ensure the implementation of the criminal policy, arising from the provisions of the Optional Protocol to the UN Convention on the Rights of the Child regarding the sale of children, prostitution and child pornography, ratified on 22.02.2007, of the Council of Europe Convention for the Protection of Children against of sexual exploitation and sexual abuse, ratified on 19.12.2011;

- implementation of the provisions of the Council of Europe Convention on computer crime, the rapid preservation of computer data and the interception of computer data;

- the implementation of the Convention of the Council of Europe on computer crime and of the Council of Europe for the protection of children against sexual exploitation and sexual abuse (Lanzarote 2007), in terms of guaranteeing the effective investigation and prosecution of the crimes provided for by the Convention;

- implementation of Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on combating sexual abuse of children, sexual exploitation of children and child pornography.

Thus, the material rules relevant to cyber security and the fight against cyber-crimes are set out in a series of acts, as follows:

1) The Criminal Code of the Republic of Moldova. Through the lens of this act, the legislators managed to regulate acts qualified as crimes in the digital environment, namely in art. 2081 the production, distribution, diffusion, import, export, offer, sale, procurement, exchange, use or possession of images or other representations of one or more children involved in explicit, real or simulated sexual activities, or of images or other representations of a child's sexual organs, represented in a lascivious or obscene manner, including in electronic form, is punishable by imprisonment from 1 to 3 years[1].

In the same way, some economic crimes regulated also through the lens of the criminal code are punished. Art. 237 states that the manufacture for the purpose of putting into circulation or the putting into circulation of false cards or other payment instruments, which do not represent monetary tokens or securities, but which confirm, establish or grant patrimonial rights or obligations, is punished with fine in the amount of 550 to 1050 conventional units or with unpaid work for the benefit of the community from 180 to 240 hours, or imprisonment of up to 5 years, and the legal person is punished with a fine in the amount of 2000 to 4000 conventional units with the deprivation of the right to exercise a certain activity, as well as the indication of the aggravating forms of this crime in paragraph (2) of the same article.

[1] The Criminal Code of the Republic of Moldova from 18.04.2002 [On-line]: http://lex.justice.md/md/331268/.

Moreover, the Criminal Code of the Republic of Moldova dedicates an entire chapter to specific informational crimes (Chapter XI. Computer Crimes and Crimes in the Telecommunications Domain). But are these limited regulations, transposed in 10 articles, sufficient to regulate the most vast and complex social formation? At art. 259 – 2611 of the Penal Code, a series of activities associated with the information space are stated which fall under the criminal law and are to be punished. These are: illegal access to secured information; the illegal production, import, commercialization or making available of technical means or software products; illegal interception of a computer data transmission; altering the integrity of computer data, disrupting computer systems and their correct functioning; illegally producing, importing, trading or making available passwords, access codes or similar data; computer fraud; computer fraud; violation of the security rules of the IT system; unauthorized access to telecommunications networks and services. At the same time, the countries of the European Union have drastically widened the spectrum of crimes that fall under the criminal law. For example, in Estonia, the Penal Code at art.1572 punishes the illegal use of another person's identity up to 3 years in prison, and art.280 of the same law punishes the presentation of false information with a fine of up to 2000 euros or with imprisonment of up to two years (aggravating forms of the crime). Even more recently, in the Criminal Code of Germany, articles 269 and 270 punish the falsification of digital records.

Analyzing the crimes included in chapter 11 of the Criminal Code, the Special Part, we distinguish the generic legal object of the crime, which is social relations in the field of IT and telecommunications. Each of the mentioned crimes has a special legal object, represented by social relations regarding legal access to data and information; social relations related to the security of information systems; social relations regarding authorized access to computer systems (Brânza, 2005, p. 493).

However, the legal framework is one in permanent development, and the reality is that at the present moment the normative spectrum of the Republic of Moldova in the matter of cyber security and combating cyber-crimes is quite limited. For example, there is no clear distinction between the types of cybercrimes, which can be divided into three broad categories, namely cybercrimes against:

- individuals - this form of crime is catching new clones in the information society, as there are currently over three billion online users on social media platforms, who are constantly interactive with information, social networks being the preferred target of criminals. And for 99% of all computers, one of the following programs is

installed: Oracle Java, Adobe Reader, Adobe Flash, which are vulnerable to cyber exploitation;

- property - just like in the real world where a criminal can steal and rob, so in the cyber world criminals resort to theft of data and information. In this case, they can steal a person's bank details and manage the funds; misuse of credit card to make numerous online purchases; using the software for illegal purposes, to gain access to an institution's databases and information or to paralyze the entity's systems, as well as stealing trade secrets or tampering with online services;

- of the state - although not as common as the other two categories, crimes against a state are often called acts of cyber terrorism. This set of crimes can wreak havoc and create panic among the civilian population. This category of crimes includes hacking government websites, military websites or distributing propaganda material, or even more serious – they can paralyze the military activities of a state and take control of remotely controlled military equipment. The perpetrators can be terrorist formations or hostile states.

The issue of cyber security and the first approaches to solving it, at the level of government policies, were exposed in the Republic of Moldova through the National Strategy for the Development of the Information Society "Digital Moldova 2020", approved by Government Decision No. 857 of 31.10.2013. Namely, the implementation of this sectoral strategic vision allowed the formulation at national level of a policy, legislative, normative, regulatory and institutional framework, which raised the national cyber security framework to a complex and functional qualitative level.

But as this dynamic sector is constantly emerging, so the state policies in this direction must be constantly developing and consolidating[1]. In this context, the Republic of Moldova must continue international cooperation, introduce new collaboration mechanisms, either through the ratification of new relevant Conventions, or in the engagement of bilateral bonds at the state level, with other countries, for joint strengthening of capacities.

The creation of specialized structures for the prevention and combating of cyber and informational criminality within the bodies of the Prosecutor's Office and the Ministry of Interior did not achieve the expected effect, because the training of specialists in the respective field is not a priority of the agenda, as a rule they are

[1] Government Decision no. 857 of 31.10.2013, regarding the National Strategy for the Development of the Information Society - Digital Moldova 2020 [On-line]: http://lex.justice.md/md/350246.

specialists in the IT field, reprofiled as investigators of the categories of nominated crimes. This fact can be easily observed through the statistical study of the results recorded in the Central Database of the authorized structures. Obviously, this category of crimes usually has a cross-border character, sometimes, certain components of information technologies are physically placed on the territory of other states, and the subjects of the crimes are strongly diverse and positioned quite securely in relation to the representatives of law enforcement bodies, advanced by the latest modern technologies. In other cases it is difficult to identify the data of the victims, who do not claim certain damages, etc. At other times, the consumer of the results of cyber, information crimes is an unidentified one, or based on certain false profiles. Of course, interstate cooperation and joint meetings, the exchange of information, between investigative agencies is the key to success in preventing and combating these categories of crimes.

3. Conclusion

Cybersecurity is the key to success in preventing and combating cybercrime. The Republic of Moldova has many deficiencies in the field of reference. The latest events in the world indicate that society has advanced quite quickly in choosing the means to achieve the proposed goals, configuring such notions as „cyber war", „cyber and informational attacks", the massive involvement of the authors of computer crimes , cyber in the electoral processes, the influence on the electoral polls and their results, through the use of false profiles and information platforms, the manipulation of public opinion or the creation of erroneous public opinion by certain exponents of interest groups organized in well-directed and coordinated teams from the shadow of such the so-called computer „trolls", equipped with the most modern information technologies, the denigration of certain public figures or who claim certain positions in the social sphere. And vice versa, polishing the image of certain dubious characters, who also threaten the security of the state, or pursue personal goals of illicit enrichment at the expense of the interests of the citizen, the Republic of Moldova has a vast and sad experience in this field, but, unfortunately, it is not always learned the lesson so as not to repeat these shortcomings in the future. Formal association with certain international structures in the field of computer criminality does not solve the problem, this is only a step towards the proposed goal. Creation of professionals, adequate remuneration for an IT specialist with a profile in jurisprudence, identification of vulnerable places in the field of cyber security and timely legislative intervention, adequate provision

with modern technologies, would be just a few solutions at the moment. As a rule, the material remuneration of specialists in the IT field is much higher than that of those employed in legal bodies, and the activity of these specialists in legal bodies is not strongly motivated, even unattractive. Time works against the proposed goal, given that the passivity of the responsible persons is accentuated, given that the Criminal Law does not cover the entire spectrum of criminal acts. And these criminal acts usually attack not only the intellectual right, other rights protected by Chapter 11 Special Part of the Penal Code, but are also interspersed with crimes from other compartments, such as crimes that attack sexual freedom, the right to property, the right to life and health, other categories of crimes.

References

Miller, L. C. (2014). *Cybersecyrity for dummies.* John Wiley & Sons, p. 13.

Brânza, Sergiu & Stati, Vitalie (2005). *Criminal Law, special part*. Chisinau, Cartier, p. 493.

*** (2002). *The Criminal Code of the Republic of Moldova from 18.04.2002 [On-line]*. http://lex.justice.md/md/331268/.

*** (2020). *Government Decision* no. 857 of 31.10.2013, regarding the National Strategy for the Development of the Information Society - Digital Moldova [On-line]: http://lex.justice.md/md/350246/.

*** (2015). *Government Decision* no. 811 of 29.10.2015, regarding the National Cyber Security Program of the Republic of Moldova for the years 2016-2020 [On-line]: http://lex.justice.md/viewdoc.php?action=view&view=doc&id= 361818&lang=1.

https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-csss/national-cyber-security-strategies-in-the-world.