ISSN (Online) 2456 -1304

International Journal of Science, Engineering and Management (IJSEM)

Vol 11, Issue 9, September 2024

Cybercrime, Prevention, and Risk Factor

[1] Adriana-Iuliana STANCU, PhD

[1] Associate Professor, Dunărea de Jos" University of Galați, Romania, Head of the Department of Legal Science, Faculty of Law and Administrative Sciences

Corresponding Author Email: [1] adriana.tudorache@ugal.ro

Abstract*— Information civilization, politics and the globalization of information and business, embracing nationalism and border-defying economic and cultural invasions, have led to the so-called "new IT order" and "IT warfare" (Infowars), electronic warfare strategies, offensives that include defense techniques, economic warfare, and psychological warfare, including the arts of information and disinformation. The main crimes committed on the Internet are related to copyright infringement - software, data, databases, etc. protection related to computer fraud, unauthorized access to computer systems and other crimes committed through communication networks. Computer crimes can be classified according to the recommendations of the Council of Europe addressed to the Member States. The reality is that most countries do not take a unified and coherent position for the application of legal provisions on the Internet. In these conditions, prevention is almost non-existent, and the risk is mostly left to the insurer.

Index Terms: Globalization; computer crimes; prevention; risk.

I. INTRODUCTION

The continuous development of information technology and the emergence of new means of communication and communication among people have had a beneficial effect on the economic, social, and political life of the world, but have also led to an increase in the number of newly registered crimes. Given that almost all aspects of society rely on computer systems, cybercrime poses a serious threat. Cybercrime is growing rapidly due to vulnerabilities in computer systems, long-distance activities, and complete destruction of evidence of the exact time and method of cybercrime. The growth of computer crime is supported by the transnational nature of the use of computer systems and networks, legal or otherwise, in situations that cross national borders. The globalization of computer networks is believed to have led to the emergence of new forms of crime, as well as international efforts to combat this scourge. to the development of consciousness. Some authors argue that cybercrime law will form a new and independent field, characterized by the expansion of laws and practices in all legal orders in recent years. However, this law shows great heterogeneity in terms of regulatory sources, models of inspiration, scope of intervention, requiring national legislatures to adopt uniform and uniform rules on computer crimes. The specific nature of cybercrime has led to the creation of agencies and agencies, public and private sector organizations working together to determine the application of regulations in this area. optimal solutions. Actions to combat cybercrime at the European Council and European Union level have led to the adoption of documents instructing national legislators to adopt uniform or harmonized rules.

II. EUROPEAN REGULATION IN THIS FIELD

At the level of the Council of Europe [1]: R/85/10 on the practical application of the Extradition Convention against the Telecommunications Surveillance Authority; R/88/2 on anti-piracy measures in the field of copyright; R/87/15 on the Regulation of the Use of Personal Data in the Police Sector; R/89/9 on the protection of personal data and computer-related crime in the telecommunications services sector, adopted on 13 September 1989[2]. The International Criminal Law Association endorsed the proposed guidelines. National legislators present at this meeting as part of the International Criminal Law Conference held in Rio de Janeiro from 4 to 10 September 1994. The Council of Europe's minimum list of recommended criminal offenses in the case of intentional acts. , which is included in Chapter II of the Congressional Resolution relating to Computer Crimes and Other Crimes Against Computer Technology and includes Section 450: Computer Fraud; computer fraud; damage to computer data and software; hacking computers; unauthorized access; unauthorized retention; unauthorized reproduction of protected computer software; Unauthorized reproduction of topography. Resolution 1 was adopted by the European Ministers of Justice at the 21st Conference in Prague in July 1997, recommending that the Committee of Ministers support the work on computer crimes carried out by the European Committee on Criminal Matters. to bring national criminal laws closer together and to allow the use of investigative techniques in relation to computer crimes. On the occasion of the 20th summit held in Strasbourg in October 1997, the problem of finding common solutions for the development of new technologies was raised through the action plan adopted by the heads of state and government members of the European Council. It is based on the norms and values of the Council of Europe. The Budapest Convention on Computer Crime was adopted on November 23, 2001, in Budapest by Act No. 64/2004452. This instrument culminated in the Additional Protocol on the Criminalization of Racist and Xenophobic Conduct by Computer Systems, signed in Strasbourg on 28 January 2003.

ISSN (Online) 2456 -1304

International Journal of Science, Engineering and Management (IJSEM)

Vol 11, Issue 9, September 2024

This convention has been ratified by many countries, even outside Europe. such as USA, Canada, Japan and South Africa453. The Convention defines nine basic crimes in Part I, namely: illegal access (art. 2), illegal access (art. 3), attacks on the integrity of data (art. 4) and computer systems (art. 5), misuse of devices (Article 2), classic crimes, computer fraud (Article 7) and computer fraud (Article 8), child pornography offenses (Article 9) and intellectual property infringement (Article 10)). The 1989 Council of Europe Recommendations or the 2001 Convention on Computer Crime have always given national legislators great deference in choosing the regulatory provisions, type, and establishment of sanctions.

On October 15, 2013, a memorandum of understanding was signed between the Council of Europe and the Government of Romania in Strasbourg, and an agreement was reached on the establishment of a Council of Europe Office on Cybercrime in Bucharest. to ensure the implementation of technical assistance projects in the area of computer crime, including joint projects with the European Union.

Through the European Union's Internal Security Strategy: five steps towards a more secure Europe, it is envisaged to increase the level of security for citizens and businesses in cyberspace. In January 2013, the European Cybercrime Center (EC3) was established to create a point of convergence in the fight against cybercrime at the European Union level. On August 12, 2013, the European Parliament and the Council adopted Directive 2013/40/EU461 on attacks against information systems and replacing Council Decision 2005/222/JHA, which defines the concept of computer data as a representation of facts, in a form suitable for processing in a computer system. information or concepts, including a program that enables a computer system to perform a function.

III. CYBERCRIME IN ROMANIA

Cybercrime is a concept that is unpredictable to some. Despite concerted efforts, we currently do not have a legal definition at the international level, a concept recognized and accepted by the Council of Europe and the United Nations. However, the lack of a generally accepted definition did not prevent this concept from entering the current vocabulary, the easy detection of computer crimes in specialized literature, law faculty, various statistical data and sometimes even in legislation. When we refer to cybercrime, we must first consider the criminal law that includes a number of criminal offenses in which a computer system or computer data constitutes the real object of the crime. That's why we sometimes talk about computer crime when a criminal's behavior damages or threatens the privacy, integrity, or availability of computer systems or computer data. Reporting on computer systems and computer data as objects of crime is not ineffective. If we refer to them as means or tools for committing crimes, there is a danger of unwarranted expansion of the concept. So, if we want to include it in the category of computer crimes, it is crime art.2 on Law no 8/1996 on Copyright and Related Rights, Common Offenses Published or Committed by Computer Systems, will certainly expand the concept of cybercrime considerably. For example, the offense of child pornography via computer networks - art. 374 para. 2 and 3 of the Criminal Code generally fall within the scope of cybercrimes. However, child pornography was first criminalized in Romania without reference to computer systems. We can also discuss harassment in the online environment - art. 208 para. 2 of the Criminal Code on violation of privacy through technical monitoring related to the use of computer systems or computer programs - art. 226 para. 1 Criminal Code, recruitment of minors in the online environment - Art. 222 Penal Code etc [4].

Despite what is presented in the doctrine, I believe that computer crime is part of several complex crimes like: computer fraud - Art. 249 Criminal Code, computer fraud - art. 325 Penal Code, illegal access to a computer system - art. 360 Criminal Code, altering the integrity of computer data (Criminal Code Section 362), disrupting the operation of computer systems (Criminal Code Section 363) or unauthorized transfer of computer data (Criminal Code Section 364) [5].

IV. PREVENTION AND RISK

Lately, most of the reported cases are ransomware incidents. These are often triggered by ignorance or carelessness on the part of employees. Data encryption or data deletion resulting in disruption of operations, as well as blackmail with ransom demands, should be highlighted. Important threats include fraud (scam), ransomware and vulnerabilities (compromise). [6].

Russia's war of aggression has brought these threats even more to the fore. The conflict in Ukraine has made threat scenarios from state actors more critical. War was not part of these patterns, and therefore no one can know how this war will spread in the digital world. These suspicions are only a few accounts that require preventive measures. There are new malicious programs in circulation such as Wiper. This is malware that destroys data and irreversibly erases electronic storage media.

This is a new reality as malware is essentially aimed at blackmail, which means it has a financial motive. If it's just destruction, it means the insurer may have to pay for the entire restoration, which is huge".

Policy is no substitute for prevention [7].

SMEs do not always respond adequately to these threats. In the consulting practice of insurance companies, it is regularly observed that risks are suppressed. Companies, which are often quite small, doubt they could be a useful target for cyber criminals. Unfortunately, this is not correct. Therefore, more information and advice are needed in this sector of insurance than is the case in other sectors. Once a

ISSN (Online) 2456 -1304
International Journal of Science, Engineering and Management (IJSEM)
Vol 11, Issue 9, September 2024

company has decided to seek advice, steps such as improving IT security or taking out cyber insurance often follow.

Customers who have never been affected by a cyber-attack are less likely to take out insurance. The better positioned an SME is in terms of cyber risk management, the greater the awareness that it is impossible to be 100% secure. This means that one is aware of the residual risk that remains despite risk reduction measures and is therefore interested in transferring this risk to the insurance industry.

Companies have also understood that the vast majority of attacks are opportunistic and that the weakest link in the chain is most likely to be affected. Companies that have solid knowledge of cyber security are more likely to take out insurance. Customers who have not yet dealt extensively with the subject or who do not have dedicated knowledge are less likely to take out insurance. The same is true for clients who are very risk averse and are prepared to take that maximum risk themselves. [8]

Checks with insurance companies are required.

Cyber insurance is also a service policy, meaning customers have 24/7 access to a crisis management team. If it is brought quickly and subsidiarily, the damage is usually less than without it. This is a huge added benefit. Companies that use insurance as a "last line of defense"—that is, not as a substitute for protective measures—at least aren't stuck with all the financial costs. Insurance always has a complementary role, but never replaces other risk management.

There is no such thing as absolute security, but steps can be taken to reduce the risks. Cyber insurance exists to cover any costs arising from the residual risk of a successful cyber-attack despite high precautions. Once a company reaches a certain size, a thorough risk assessment is conducted. Insurers who do not meet the minimum standards will not make an offer. "This is often an impetus for corporate customers to think critically about their own security measures.

In the area of IT security, we talk about so-called cyber hygiene, which is essential for protecting a company from cyber-attacks. This includes, for example, security updates, employee training and, in particular, ensuring harmless, complete and readable data backups. In the event of a cyber-attack, cyber insurance customers are supported with a team of specialists and are offered immediate professional help. This ensures, among other things, that the SME can resume operations as quickly as possible in the event of an interruption.

Preventive measures do not have to be reported, so it is not possible to determine which measures had a positive effect on which damage occurred and which consequences of the damage. This could be a starting point, the interest of SMEs, in the sense of reporting these measures so that they can be generalized as mandatory and thus, to ensure the continuation of operations, great attention should be paid to the topic of prevention.

V. CONCLUSIONS

In order to address these issues, we must broaden our scope of work through the creation of novel investigation methods, the use of state-of-the-art analytical instruments, or the formation of fresh community collaborations. This is because we must adjust to the ever-changing nature of the cyber threat.

Multiple field offices require specially trained cyber teams to collaborate with task force partners supported by the government-established express agency.

To respond to significant incidents, the Rapid Response Cyber Action Team can deploy across the nation in a matter of hours.

One can collaborate closely with our international counterparts to pursue justice for victims of malicious cyber activity in the relevant areas, since cyber legal assistants are stationed at Romanian embassies or representations.

The public may submit reports of online crimes to the government agency that was specifically established for this purpose. The loss recovery team can assist in freezing important cash for victims of cybercrime by using such complaints.

A watchdog organization and the government agency can help monitor events around-the-clock and stay in touch with field offices throughout the nation.

Asset forfeiture is a potent weapon that law enforcement uses to take away the property and gains that criminals and criminal organizations have obtained via illegal means. Additionally, it's employed to pay back crime victims.

By implementing the necessary security precautions, such as being vigilant and aware when logging in, which are essential to preventing cyber intrusions and online crimes, individual actions may also be made to contribute to a decrease in the crime rate in the field. All of this is done to safeguard your personal data, your computer, and the networks you use.

Summer courses for adults can be arranged within regional institutions, covering beginning courses at the secondary education level, as it is vital to have some understanding of both crime and internet threats.

Business email compromise scams, one of the most financially destructive types of online fraud, take advantage of the fact that a large number of us transact business via email, both personally and professionally.

Identity theft is the act of someone stealing personal data, like your Social Security number, and using it for fraudulent or theft purposes.

Malicious software, sometimes known as malware, known as ransomware locks you out of your computer's files, networks, and systems and typically demands a ransom to unlock.

Phishing and spoofing are tactics used by con artists to deceive victims into providing sensitive information.

Particularly for young people, internet predators pose an

increasing hazard, so it is important to educate them on this matter.

In addition, a hotline for victims of online or Internet crimes must be established; as previously stated, a subsequent complaint is also required. For the purposes of intelligence gathering and investigation, crime reports or complaints are used. Quick reporting can also aid in the recovery of money that have been misplaced.

Every user of a connected device must be aware of and cautious against the more sophisticated cybercrimes and intrusions made possible by the internet.

It is imperative to install a robust and reliable antivirus program in order to keep the systems and software up to date.

Using a public WiFi network to make any kind of purchase that requires the usage of personal information is risky. Every online account must have a strong, one-of-a-kind passphrase, and those that support it must be set up with multi-factor authentication.

All correspondence must include a verified email address, especially when responding to an invitation by visiting the website. Unknown emails should not be opened, and when accessing social media accounts, caution should be exercised in paying attention to any requests for payments or collections as this could provide information that could lead to the identification of those who are breaking the law.

In a digitally connected world, we can only attain safety, security, and trust by working together.

VI. ACKNOWLEDGEMENT

The paper was achieved within the project unfolded by "Dunărea de Jos" University of Galati entitled: "Developments and Perspectives in Contemporary Law", financing Contract no RF2469/31.05.2024.

REFERENCES

[1] A.M. Weber, The Council of Europe's Convention on Cybercrime, în Berkely Technology Law Journal, vol. 18, 2003, p. 425 și urm.

[2] J. Clough, A World of Difference: The BudapestConvention on Cybercrime and the Challenges of Harmonisation, în Monash University Law Review, vol. 40, 2014, p. 698 și urm.;

[3] C. Rotaru, Comentariu, în C. Rotaru, A.-R. Trandafir, V. Cioclei, Drept penal. Partea specială II, ed. 4, Ed. C.H. Beck, București, 2020, p. 347-348.

[4] G. Bodoroncea, V. Cioclei, I. Kuglay și colab., Codul penal. Comentariu pe articole, ed. 3, Ed. C.H. Beck, București, 2020, p. 919-920.

[5] Dubber, Markus. (2011). Codul Penal Model al Institutului American de Drept și Dreptul Penal European. În André Klip (Ed.), Dreptul penal substanțial al Uniunii Europene.p. 87-88

[6] Boas, Gideon, James L. Bischoff, Natalie L. Reid și B. Don Taylor III. (2011). Procedura penală internațională, volumul 3. Cambridge University Press.p.34-35

[7] Maras, Marie-Helen. (2014). Computer Forensics: Cybercriminals, Laws, and Evidence, Ediția a doua. Jones și Bartlett.

[8] Maras, Marie-Helen. Cyber Law and Cyber Freedoms. Oxford University Press, 2020, p.67