Sergiu Cernomoreț
Andrei Nastas

Comparative Analysis of Cybercrime in the Criminal Law System

ADJURIS
International Academic Publisher

Comparative Analysis of Cybercrime in the Criminal Law System

Andrei NASTAS

Activity

Andrei Nastas is PhD in law, associate professor at Transfrontier Faculty, "Lower Danube" University from Galați (România), scientific researcher at the Institute of Legal, Political and Sociological Research of the Academy of Sciences of Moldova, where he is specialized in criminal law, criminal procedural law, criminology and forensics. Likewise, he is a lawyer and mediator within the "Advice-Group" Associate Law Firm, specializing in criminal and contravention cases. He is a member of the following research projects: „the quality of the judicial act and the respect of the rights of the person in the Republic of Moldova: interdisciplinary research in the context of the implementation of the association agreement between the Republic of Moldova and the European Union" (research project, project code - 20.80009.1606.05, participation period 2020-2023); „transfrontier and interdisciplinary approaches regarding the quality of life" (financing contract no. RF 3624/30.09.2021, conducted within the Transfrontier Faculty, "Lower Danube" University in Galați, România, 2022); „Moldova Higher Education" Project (P167790, IDA Credit No. IDA-65420, Title of Consulting Services: Develop qualification standards for the general field of study 103 Security services for Higher Education, 2023). Member of the editorial board of prestigious scientific journals in the field of legal sciences: WASET Scientific and Technical Committee & Editorial Review Board on Law and Political Sciences; American Yearbook of International Law (AYIL); International and European Union Legal Matters (INTEULM); Juris Gradibus Journal. Editor of prestigious journals in the field of legal sciences: *Across*, *Legea și Viața*, *National Science*.

Publications

Author of several scientific works in the field of criminal law, criminology, as follows: 35 scientific articles published in prestigious journals in the legal field, 2 monographs („*Răspunderea pentru declarațiile cu rea-voință în dreptul penal*", Bucharest, Pro Universitaria, 2022; „*Infracțiunile privind traficul ilicit de droguri*", Bucharest, ProUniversitaria, 2022); university courses in co-authorship („*Încadrarea juridică a infracțiunilor privind traficul ilicit de droguri*", Chișinău; „*Managementul securității și ordinii publice*", Chișinău; „*Particularitățile calificării juridice a infracțiunilor economice*" Chișinău); Criminology Treaty, Chișinău, 2022 (in co-authorship); Criminology Treaty, Pro Universitaria, Buchares, 2023 (in co-authorship).

Sergiu CERNOMOREȚ

Activity

Sergiu Cernomoreț is PhD in law, associate professor at Transfrontier Faculty, "Lower Danube" University from Galați (România), scientific researcher at the Institute of Legal, Political and Sociological Research of the Academy of Sciences of Moldova, where he specializes in criminology, contravention law, criminal execution law. Likewise, he is a lawyer and mediator within the "Advice-Group" Associate Law Firm, specializing in criminal and contravention cases. He is a member of the research project „Moldova Higher Education" Project (P167790, IDA Credit No. IDA-65420, Title of Consulting Services: Develop qualification standards for the general field of study 103 Security services for Higher Education, 2023) and editor of prestigious journals in the field of legal sciences.

Publications

Author of several scientific works in the field of criminal law, criminology, as follows: 2 monographs („*Răspunderea penală pentru samavolnicie*", Pro Universitaria, Bucharest, 2022; „*Infracțiuni privind traficul de droguri și investigarea criminalistică a traficului de ființe umane*", Pro Universitaria, Bucharest, 2022); Criminology Treaty, Pro Universitaria, Buchares, 2023 (in co-authorship).

Sergiu Cernomoreț
Andrei Nastas

Comparative Analysis of Cybercrime in the Criminal Law System

ADJURIS
International Academic Publisher

Bucharest, Paris, Calgary 2023

ADJURIS – International Academic Publisher
This is a Publishing House specializing in the publication of academic books, founded by the *Society of Juridical and Administrative Sciences (Societatea de Stiinte Juridice si Administrative)*, Bucharest.
We publish in English or French treaties, monographs, courses, theses, papers submitted to international conferences and essays. They are chosen according to the contribution which they can bring to the European and international doctrinal debate concerning the questions of Social Sciences.
ADJURIS – International Academic Publisher is included among publishers recognized by **Clarivate Analytics (Thomson Reuters)**.

ISBN 978-606-95862-1-1 (E-Book)

Editing format .pdf Acrobat Reader
Bucharest, Paris
2023

www.adjuris.ro
office@adjuris.ro

Table of Contents

List of acronyms

BJS - Bureau of Justice Statistics
CAN-SPAM - Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act of 2003
EC - European Commission
CFAA - Computer Fraud and Abuse Act
CIA - Central Intelligence Agency
CP - Criminal Code
DDoS - Distributed Denial of Service attacks
EUROJUST - European Union Agency for Criminal Justice Cooperation
EUROPOL - European Union Agency for Law Enforcement Cooperation
FBI - Federal Bureau of Investigation
FRONTEX - European Border and Coast Guard Agency (fr. Frontières extérieures)
IC3 - Internet Crime Complaints Centre
IGP - Inspectorate General of Police
INI - National Investigation Inspectorate
OECD - Organisation for Economic Cooperation and Development
NASA - National Aeronautics and Space Administration
NCSI - National Cyber Security Index
RM - Republic of Moldova
SSN - Social Security Number
USA - United States of America
EU - European Union

Introductory considerations

Importance of the topic. In recent decades, information technology has advanced significantly, leading to an increase in cybercrime. These include a wide range of illegal activities such as hacking, phishing, online fraud, cybercrime and more. As a result, cybercrime has become a major issue for the contemporary criminal law system.

Cybercrime is a growing phenomenon in today's digital world, and its consequences can be devastating for individuals and companies. As a result, the criminal law system has developed to combat these crimes and to try to protect society against them.

The development of computers has had, and still has, a major impact on everyday life, on the way business is conducted, on the way information is managed, etc. At the same time, the development of technologies has also led to the emergence of new, highly sophisticated crimes, namely cybercrime. There are many types of such crimes, including computer fraud, computer sabotage, computer forgery, etc., with software piracy accounting for the largest share of these crimes. Criminals in this field, especially hackers, use highly sophisticated software, which makes it virtually impossible to detect them and their attacks cause irrecoverable damage to companies. Computer networks have thus come to occupy a world of their own, in which criminals are in charge, and justice, for the time being, is far removed from this world.

Technological development and the widespread use of information systems has brought with it a number of risks. The increasing dependence of businesses, public institutions and even individual users on the IT systems that largely manage their resources makes them increasingly vulnerable to the impact of cybercrime.

There are many international methods and practices to prevent and combat cybercrime. These include international collaboration, standardisation of investigative practices, use of specialised technology, improved investigative capacity and better legislation.

It is important to recognise that cybercrime is a global phenomenon that requires an international approach and cooperation between governments and law enforcement organisations in order to be effectively prevented and combated.

The aim of this scientific study is to carry out a comparative analysis of cybercrime in the modern and contemporary criminal law system.

The comparison of cybercrime in the contemporary and modern legal system is a relevant and topical research topic in the context of rapidly evolving technology and the growth of cybercrime globally.

The research objectives are:

- cybercrime research in the modern period;
- investigating cybercrime in the contemporary period;

- comparative analysis of the information researched, according to period (modern and contemporary), type of cybercrime, number of cybercrimes, etc.;
- description of national and international experience of cybercrime and comparison of these data;
- establishing prevention measures and recommendations to avoid cybercrime.

Research hypotheses. "The number of cybercrimes is much higher in the contemporary period compared to the modern period." "The typology of cybercrime is much more varied in the contemporary period compared to the modern period".

This paper will analyse and compare the contemporary criminal law system with the modern one in terms of dealing with cybercrime. It will examine how criminal laws and procedures have changed over time to address these crimes and how these changes have been implemented in practice.

Scientific-methodological basis. Among the best-known scientists who have researched the field of cybercrime, whose views and opinions formed the scientific and theoretical basis of the study, include: Sfetcu N., Florescu V., Popov M., Crâlov V.V., Moțcobili I., Crijanovschi S., Brajnic S.D., Begu V., Adrian Cristian M.M., Rolland Hollinger, etc. Also, for research and analysis ofcybercrime worldwide, the Council of Europe Convention on Cybercrime, adopted in Budapest on 23 November 2001, was analyse. On a national level, it was analysed the Criminal Code of the Republic of Moldova, Chapter XI Cybercrimes and Offences in the Law on Informatics, adopted by the Parliament of the Republic of Moldova, the Moldova on 22.06.2000 and the Law on Computerisation and Information Resources of adopted by the Parliament of the Republic of Moldova on 21.11.2003, etc.

Scientific research methodology. In the process of the research carried out, such methods as analytical, systemic, historical, comparative, logical-legal and deductive methods, etc. were used. The theoretical aspects of the given study are based on direct research of bibliographic sources.

The novelty and scientific originality of the obtained results derive from the fact that the study carried out is a comparative analysis, an attempt to compare cybercrime in the modern legal system with the contemporary one, both in the Republic of Moldova and globally.

Finally, this study will provide an assessment of how the criminal law system approaches cybercrime and will explore the possibilities to improve this approach. It will also examine ways of preventing cybercrime.

Chapter I.
Theoretical Aspects of Cybercrime in the Contemporary and Modern Criminal Law System

1. Definition and characteristics of cybercrime

Cybercrime is on the rise, being in the age of modern technologies, it affects all spheres of life. More and more processes are being digitised, which makes life easier but also puts us at risk. We are certainly living in a time when the simultaneity made possible by the internet offers us the opportunity to experience a revolution in communication, social relations and consumption. We live in an age of websites and fast-paced information technology development. Given this, it is undeniable that relationships established in the virtual environment lack the legal analysis through sociological and jurisdictional perspectives that technology encourages us to investigate.

The modern consumer is increasingly searching, accessing the internet to make numerous commercial transactions, and this is due to a number of factors, such as: optimising available time, trying to maintain privacy, the range of price searches, etc. Given these changes, the development of research on criminal law and the information society is essential in order to establish a new perspective on crimes whose roots lie in cyberspace or whose vicious effects of rights violations will echo in cyberspace. The study carried out, allows us to identify a number of latent weaknesses, triggered by the use of technologies aimed at the dissemination of information and knowledge through ICT, which in the analysis proposed by this research are in the inherent transformation of criminal law.

Breaking cyber security laws and rules to gain access to computer systems or data is called computer crime or cybercrime. These can take many forms, including hacking, phishing, malware, online fraud, online harassment and other illegal activities involving the use of technology. In general, these crimes are committed by individuals or groups of individuals seeking to make financial gain or disrupt the activities of an organisation or country.

In attempting to define cybercrime, reference will first be made to the existing literature.

As V.V. Krilov[1] notes, the specialist literature and the media in recent years have been flooded with different terms characterizing the new phenomenon associated with criminal activities in the field of information technology, and the terminological differentiation indicates not only society's concern about the new threat, but also the absence of a uniform perception of the essence of this threat.

The "computerisation" of social life and the "technologisation" of criminals have created the prerequisites for the emergence (or grafting of the "classic"

[1] Krilov, V.V. *Investigation of crimes in the sphere of information*. Moscow: Gorodets, 1998, p.156.

elements of crime) of a new form of crime (in general), cybercrime.[2]

The notion of "computer crime" was first proposed by a group of experts from the Organisation for Economic Co-operation and Development in Paris in 1983 and is defined as: "any illegal, unethical or unauthorized conduct affecting automatic data processing and/or a data transmission".[3]

The term cybercrime covers not only actions committed with the use of modern technology, but also a variety of informational-psychological exposures (effects) that are carried out using modern information technologies and, primarily, the media to achieve criminal ends.[4]

The same reasoning is contained in the definition proposed by S. Crijanovschi, who states that possible computer crimes (or computer crimes in the broad sense) are those that can be committed without the use of computer technologies. In this context, the author gives the example of "insult via the Internet". In other words, computer crime in the broad sense means any crime in which a computer or computer network is the object of a crime, or in which a computer or computer network is the instrument or medium of a crime.[5]

In the doctrine, a definition of the concept under discussion is also emerging in a narrow sense. In this sense, a computer-related crime is any crime in which the perpetrator interferes, without authorisation, with automatic data processing processes.[6]

In an attempt to define the notion of cybercrime a group of authors have classified the distinct views in the literature into three groups, namely:

1. Cybercrime in the broad sense (cybercrime) - criminal behaviour committed with the use of and/or on computer information, computers, computer systems or their network;

2. Computer-related crime - the socially dangerous act provided for by criminal law, the object and/or means of committing which is computerised information.

3. Computer crime in the narrow sense - the act provided by criminal law, the object of which is computer information.[7]

Furthermore, at the 10th United Nations Congress on Preventing and Combating Crime, two definitions were developed at a workshop:

---

[2] Ioniță, G. I., *Cybercrime offences: criminalisation, investigation, prevention and combating*. Bucharest: Universul Juridic, 2011, p. 9

[3] Motskobili, I., *Hackers are striving for world domination*. in: Komersant – Daily, 1998, no. 73, p.11

[4] Popova, V. I. (ed.)., Object-structural analysis of organized criminal activity in the field of private investment: textbook, Moscow, 1997. p. 19.

[5] Crijanovschi, S. *Some aspects of comparative legal-criminal analysis of computer crimes in the criminal law of the Republic of Moldova and Romania*. In: Studia Universitatis Moldavia. Series "Social Sciences", 2016, no. 3(93), p.40

[6] Introductory guide to the application of legal provisions on cybercrime / Ministry of Communications and Information Technology, Bucharest, 2004, p. 51.

[7] Vekhov, V.B., Golubev V.A., *Investigation of computer crimes in the CIS countries*: monograph, ed. B.P. Smagorinsky. Volgograd: VA Ministry of Internal Affairs of Russia, 2004, p. 56.

- cybercrime in the narrow sense is that crime which covers any illegal behaviour committed through electronic operations directed against the security of computer systems and the data processed by them;

- computer crime in a broader sense, which is any illegal conduct committed through or in connection with a computer system or network, including such crimes as: illegally possessing, providing or distributing information through a computer system or network[8].

Thus, it is argued that these definitions are not only about computer systems and networks, but also about the data they process and the information they distribute.

The legislation of the Republic of Moldova establishes criminal liability for illegal access to computer information in Article 259 of the Criminal Code of the Republic of Moldova, and for illegal interception of computer data transmission in Article 260^1 of the Criminal Code of the Republic of Moldova.

At the 10^{th} United Nations Congress on the "Prevention of Crime and the Treatment of Offenders", the term cybercrime is defined as "an act provided for by criminal law, committed with intent, by a person or a group of persons, using a computer, and by means of wire communication, committing a socially dangerous act that harms a person, a company or the interest of the State".

It should be noted that a computer crime nowadays can be committed not only through the computer itself, which is used in daily activities, but also through the variety of mobile (cellular) communication devices and communication systems.

According to the same source, computer data means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program capable of causing a computer system to perform a function.

Computer-related crime means: 'any crime in which a computer or computer network is the object of a crime, or in which a computer or computer network is the instrument or environment of a crime'.

Computer crime in the narrow sense means: "any crime in which the perpetrator interferes, without authorisation, with automatic data processing".

The main characteristics of computer security crimes are:

- high level of latency;

- the possibility of committing cybercrime remotely, sometimes even from another continent;

- participation of organised criminal groups;

- speed of criminal intent. Unauthorised access is often carried out in a short time (up to 1 minute);

[8] Marco Gercke, *Understanding cybercrime: phenomena, challenges and legal response*, ITU 2012, p. 11.

- imperfection of legislation. In the field of information processing technologies, legislation often fails to keep pace with the development of technology and training of prosecution authorities is insufficient to deal with the problems of detecting and controlling this new type of crime;

- the difficulty of establishing the crime;

- the difficulty of identifying the offender;

- the difficulty of collecting and legally consolidating evidence of cybercrime;

- the presence of a specific subject - most often a highly intelligent person, an IT professional.[9]

The following characteristics of cybercrime in the Republic of Moldova have been drawn from assessments of criminal groups operating in the field:

- organisation of the groups acting, structuring and specialisation of their members;

- the use of young people with skills in the use of computers and new technologies, who are organised and coordinated by the leaders of the criminal groups;

- a shift from computer fraud, where trust was the primary element in carrying out transactions, to frauds where the use of computer software in fraud predominates;

- the transnational nature of these offences, in the sense that victims from other countries are targeted, certain activities are carried out from other countries or computer systems from other countries are used;

- the constant concern to identify new ways of operating, to identify products that can be fraudulent and computer systems that can be compromised;

- the reorientation of criminal groups towards the fraud of electronic means of payment offered by financial institutions in the Republic of Moldova;

- reorientation of criminal groups committing computer fraud from petty fraud (small losses) against individuals to large fraud (large losses of hundreds of thousands/millions of euros) against companies;

- zoning of offenders by type of crime and country of destination, due to the specificity of the area (tourist areas, areas with a high number of well-organised criminal groups, etc.).[10]

From the *category of enablers of cybercrime that largely depend on the human factor*[11], the following can be listed:

- use of online payment measures in unsecured work environments;

- providing secret data when accessing websites of dubious origin;

---

[9] Brazhnik, S.D., *Crimes in the field of computer information: Educational method. development according to a special course* / Comp. S.D. Hawkmoth. Yaroslavl: Yarosl. state Univ., 2000, p. 28.

[10] Begu, V., *Cybercrime*, http://www.academia.edu/9204220/CRIMINALITATEA_INFORMATIC%C4%82, consulted on 1.10.1023.

[11] Milodin, D., Sbora C., *Non-security - premise of cybercrime. Theoretical and applied economics*. Volume XIX (2012), No. 4(569), p. 50.

- not using sites dedicated to certain activities and which have a high degree of certification;

- not verifying information provided by online sellers: phone numbers, email addresses;

- making payments in advance without confirmation of the delivery of products;

- providing additional information by the buyer, if it is not necessary to validate the transaction.

An attack on a computer system is carried out through the following steps:

1. Search the computer system for information. The first step in a computer attack is to search the computer system to obtain important information that can be used in the attack. It is therefore important to obtain information, such as the type of hardware used, software version, personal information of users, which can be used in the next step. Useful actions in obtaining information include: "ping sweeps" (a method of scanning the network) to determine if the target computer system is responding; port scans to see which ports may be open; queries that send error messages back to the system when a transmission problem has been detected; password guessing.

2. Breaking into the computer system. As soon as the target computer system has been identified and information about it has been gathered, the next step is to launch the attack in order to penetrate the system.

3. Changing the settings of the computer system. Changing the computer system settings is the next step after logging into the computer system. This step allows the attacker to re-enter the compromised computer system more easily.

4. Communication with other systems. Once the network or computer system has been compromised, the attacker then uses it to attack other networks and computers. The same tools that are used in step 1, are now targeted at other systems.

5. Affecting networks and devices. This step includes deleting or modifying files, stealing valuable data, destroying computers, or Denial of service attacks (DOS)[12].

Another way of computer attack **would be the use of computer viruses**, which in turn are nothing more than software created by an IT specialist that penetrates a computer system without the owner's knowledge. Usually, a virus attaches itself to a file so that the virus runs in memory or in the operating system every time the system executes the infected file. The effects of viruses can be benign, such as periodically displaying a funny message, but can also have very serious effects such as the permanent loss of information on the computer or the destruction of the memory storage drive. Any program that multiplies without the

[12] Moise, Adrian Cristian, *Methodology of forensic investigation of computer crimes*, Universul Juridic Publishing House, Bucharest 2011, p. 142.

user's consent is a virus.

Malicious viruses (**malware**) are classified into hardware viruses, which affect hard disk and memory, and software viruses, which affect files and programs in memory or on disk, including the operating system or its components.

A Trojan horse is a type of spyware, which appears to do something useful, but in reality, allows files to be deleted or modified, files to be sent over the network to the attacker, or other programs and viruses to be installed on the computer system.

Botnets belong to the category of malicious programs that make profit through their actions. Thus, Trojan Horse, Worm and Virus are programs that allow the infected computer to be placed under the remote control of an attacker.

The infected computer is known as a "zombie." When hundreds, thousands or even tens of thousands of zombie computers are under the control of an attacker, the attacker creates a botnet.

The investigation of computer fraud does not differ much from the investigation of traditional crime, but can sometimes become much more complex [13]. The objective of the work carried out by the prosecution authorities, as a phase of the criminal process, is to gather the necessary evidence on the existence of the crime, to identify the perpetrators and the victims and to establish the liability of the perpetrators.

Who are the criminals? Information security offenders can fall into various categories, committing more or less serious crimes, broadly categorised into individuals within an organisation and incidents and outsiders - who are a major source of risk because they are more difficult to detect and investigate than those within organisations. For a more specific approach these two major categories of offenders, depending on the specifics of their activity and how they use the information, can be divided into smaller segments such as employees, consultants or system maintenance staff, suppliers or customers, competitors, hackers or professional criminals, espionage experts, accidents or natural disasters.

One category of particular interest is that of outsiders, namely hackers.

Hackers are computer enthusiasts who usually aim to "crack" certain codes, databases, websites, etc. Hackers are divided into amateurs and professionals.

Amateur hackers are those who attack random targets wherever and whenever they get the chance. For the most part, their actions are fun. For example, increasingly frequent attacks on Yahoo and Hotmail have blocked search engines and their respective email accounts for several days, resulting in millions of dollars in damage. These amateur hackers are the only ones to face justice. The reason is simple. Those real hackers who can write their own programs are usually clever enough to make certain schemes that mislead anyone who would try

[13] Talpă, Boris, *Brief incursion into the characteristics of computer crimes*, https://juridicemoldova.md/6987/scurta-incursiune-in-caracteristica-criminalistica-a-infractiunilor-informatice.html, consulted on 1.10.2023.

to determine the source of the attack.

Professional hackers are those who have extensive domain knowledge, experience and usually work in groups. Their usual targets are important systems that have advanced protections and contain top secret information, such as Pentagon or NASA databases. Once obtained, these files (information) are published all over the Internet for as many people as possible to view or use. Any true hacker must abide by a "Hacker's Code of Laws", which is well established, known and respected.

One of the best known hacker groups is "Anonymous". Members of this group can be recognised by the Gay Fawkes mask. Their actions include numerous website hacks, often directed against state institutions and even the Vatican. The latest major operation was the hacking and publication of 5000 accounts of members of the Islamic State terrorist group in response to the Paris attacks in November 2015.

Crackers. One particular type is crackers, they represent a particular style of hacker, who specialise in "cracking" shareware programs, or requiring a particular serial code. The only people who are harmed by this category of hackers are those who write and design "cracked" programs. The protection systems of these applications can be "defeated" in two ways:

- enter the code, which can be found either on the Internet or using a program similar to OSCAR 2000, which is a code library.

- the second method is used for more advanced protection systems, which require hardware keys (which are installed on the computer's parallel ports and send a coded signal whenever requested by the software program), are patches. They are programs that are made specifically for certain software applications, which once launched modify the executable code, inhibiting instructions that require the hardware key.

Patches and serial code libraries are most often found on the Internet. They are made by certain people (who are sometimes former employees of the companies that wrote the software in question) who just want to damage the designing company. However, it is very rare to find those who place patches and serial code on the Internet.

2. History and evolution of cybercrime in the modern and contemporary criminal law system

The development of information technology and information systems, which is in a state of rapid and constant change, has made its mark on all areas of social, economic and civil life, etc., decisively influencing the progress of humanity. In addition to the benefits it offers, this true 'cyberspace' also poses a huge risk of cybercrime.

The first cybercrimes ranged from theft and misuse of information, from credit card numbers and personal data to file sharing of various goods - music,

video or child pornography. The history of hacking dates back to the 1950ˢ, when a group of phreaks (short for "telephone crazies") began hijacking portions of the world's telephone networks, making unauthorized long-distance calls and creating special "party lines" for colleagues. With the proliferation of computer bulletin board systems (BBS) in the late 1970ˢ, the informal phreaking culture began to coalesce into organized groups of individuals who joined the telephone network to "hack" corporate and government computer network systems.

Although the term hacker predates computers and has been used since the mid-1950s in connection with electronic hobbyists, the first recorded example of its use in connection with computer programmers who were skilled at writing, or "hacking," computer code was in a 1963 article in a student newspaper at the Massachusetts Institute of Technology (MIT). After the first computer systems were connected to multiple users via telephone lines in the early 1960ˢ, hacking came to refer to individuals who gained unauthorized access to computer networks, either from another computer network or, as personal computers became available, from their own computer systems. Most hackers were not criminals in the sense of being vandals or seeking illicit financial rewards. Instead, most were young people driven by intellectual curiosity; many of these people went on to become computer security architects. However, because some hackers sought notoriety among their peers, their exploits led to outright crimes. In particular, hackers began breaking into computer systems and then bragging about their exploits, sharing stolen documents as trophies to prove their bragging. These exploits have grown as hackers have not only penetrated, but sometimes taken control of government and corporate computer networks.

One such criminal was Kevin Mitnick. He allegedly hacked into the North American Aerospace Defence Command (NORAD) computer in 1981, when he was 17, an exploit that highlighted the seriousness of the threat posed by such security breaches.

Concern about hacking contributed first to a review of federal sentencing in the United States, with the Comprehensive Crime Control Act of 1984 and then the Computer Fraud and Abuse Act of 1986.[14]

The extent of cybercrime is among the most difficult to assess, as victims often prefer not to report crimes - sometimes out of embarrassment or fear of subsequent security breaches. Officials estimate, however, that hacking costs the global economy billions of dollars annually. Hacking is not always an outside job - related criminal activity involves individuals within corporations or government bureaucracies deliberately altering database records either for profit or for political objectives. The biggest losses come from theft of proprietary information, sometimes followed by extortion of money from the original owner for the return of the data. In this sense, hacking is old-fashioned industrial espionage by other means.

[14] All about hacking, https://www.britannica.com/topic/cybercrime/Hacking, consulted on 1.10. 2023.

The history and evolution of cybercrime is easy to follow and coincides with the evolution of the internet itself. The first crimes were, of course, simple hacks to steal information from local networks, but as the Internet became more established, so did the attacks.

While cybercrime existed before that, the first major wave of cybercrime came with the proliferation of email in the late 1980s. It allowed a range of scams and/or malware to be delivered to your inbox.

The next wave in the timeline of cybercrime history came in the 1990s with the advancement of web browsers. At that time there were a multitude to choose from, far more than today, and most were vulnerable to viruses. Viruses were delivered through Internet connections whenever questionable websites were visited. Some made your computer run slow, others caused annoying pop-up ads to clutter your screen or redirect you to the most unpleasant porn sites.

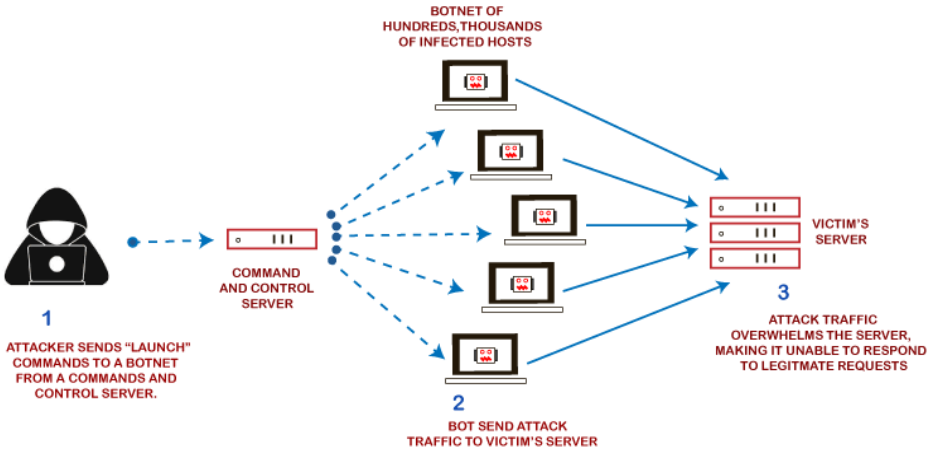
The exact origin of cybercrime, the first instance of someone committing a crime over a computer network, is impossible to know. What is possible to know is the first major attack on a digital network and then this can be used as a benchmark event in the evolution of cybercrime.

Computer viruses. The deliberate release of malicious computer viruses is yet another type of computer crime. In fact, this was the crime of choice of the first person to be convicted in the United States under the Computer Fraud and Abuse Act of 1986. On November 2, 1988, a Cornell University computer science student named Robert Morris released a software "worm" on the Internet from MIT (as a guest on campus, he hoped to remain anonymous).

This "worm" was an experimental self-propagating and replicating computer program that took advantage of flaws in certain email protocols. Due to a flaw in its programming, rather than just sending copies of itself to other computers, this software continued to replicate on each infected system, filling up all available computer memory. Before finding a solution, the virus shut down about 6,000 computers (one tenth of the Internet at the time). Although Morris's worm cost time and millions of dollars to fix, the event had few commercial consequences, because the Internet had not yet become a fixture of economic affairs. The fact that Morris's father was head of computer security for the US National Security Agency led the press to treat the event more as a high-tech drama than a foreshadowing of things to come. Since then, increasingly damaging viruses have been cooked up by anarchists and misfits in locations as diverse as the United States, Bulgaria, Pakistan and the Philippines.

DDoS attacks. On February 7, 2000, "mafiaboy", a 15-year-old Canadian hacker, orchestrated a series of denial of service (DDoS) attacks against several e-commerce sites, including Amazon.com and eBay.com. These attacks used computers in multiple locations to attack sellers' computers. The attacks crippled Internet commerce, with the FBI estimating that the affected sites suffered $1.7 billion in damage.

Fig. 1. DDoS Attack Scheme



Source: https://dnsc.ro/citeste/recomandari-gestionarea-atacurilor-ddos

Fig. 1. illustrates the pattern of a DDoS attack. Thus, by the 2000s, cybercrime had moved from being a problem of individual misconduct to a national security issue.

One of the largest known cases of computer hacking was discovered at the end of March 2009. It involved government and private computers in at least 103 countries. The global spy network known as GhostNet was discovered by researchers at the University of Toronto, who were asked by the Dalai Lama's representatives to investigate the exiled Tibetan leader's computers for possible malware. In addition to finding that the Dalai Lama's computers had been compromised, the researchers discovered that GhostNet had infiltrated more than a thousand computers worldwide. The highest concentration of compromised systems was in his embassies and foreign affairs offices located in South and Southeast Asian countries. The computers were apparently infected by users opening email attachments or clicking on web page links. Once infected with the GhostNet malware, computers began infecting files across the local network - even turning on cameras and video recording devices for remote monitoring. Three control servers running the malware were located in China's Hainan, Guangdong and Sichuan provinces, and a fourth server was located in California.

Since we are looking at the modern and contemporary period, the information will be grouped as follows:

Over time, cybercrime has undergone considerable evolution, with several stages characterising this phenomenon:

Modern criminal law includes the following periods:

1. characteristic of the 1970s - 1980s: when software piracy and credit card counterfeiting began;

2. specific to the 1980s - 1990s: it was favoured by the emergence of local and wide area networks and bridges, and characterised by major hijackings and hacker "exploits" accessing the computers of NASA, CIA and any other target that represented a political-technological symbol or an element of the powerful US military-industrial complex.

Contemporary criminal law includes the following periods:

1. specific to the 1990s and 2000s: which coincided with the proliferation of information systems and communication networks (the Internet in particular) and was characterised by the specialisation of criminals, the emergence of "real" professionals in piracy, embezzlement and computer sabotage;

2. characteristic of the years 2000-2020: fostered by the fact that information systems have penetrated all sectors of social life and control the most important of them (transport, defence, etc.), and which is characterised by the emergence of new and serious threats such as cyber-terrorism, cyber-warfare, etc.

3. After 2020, the COVID-19 pandemic - the period when cybercrime increased dramatically from digitisation to the explosion of cybercrime.

The intensive use of computers has created new opportunities for crime. Roland Hollinger[15] divided the computer crime period into four stages:

1. the period of discovery of the possibility of committing computer crime (1946-1976);

2. criminalisation of computer crime (1977-1987);

3. demonisation of computer criminals (1988-1992);

4. current period (1993 to present).

Awareness of the social danger of cybercrime has led to its criminalisation in many countries around the world. The concept of "computer-related criminal law" has thus emerged, reflecting the many new elements introduced into criminal law by new forms of crime based on modern technology.

Legislation in the field of cybercrime has followed several "waves" since the 1970s:

1. the first "wave" was driven by the need to protect the right to privacy. Laws on the protection of the individual from the processing of personal data have been adopted in Sweden (1973), USA (1974), Germany (1977), Austria, Denmark, France and Norway (1978), Belgium, Spain, Switzerland (1992), Italy and Greece (1997).

2. the second "wave" relates to the repression of economic crime, producing legislative changes in the USA and Italy (1978), Australia (1979), the UK (1981), or Switzerland (1994) and Spain (1995).

3. The third series of regulations is related to legislative intervention to protect intellectual property in the field of information technology, in countries such as the USA (1980), Hungary (1983), Germany, France, Japan, Great Britain

[15] Mafia Boys cybercrime, https://www.wired.com/2007/02/feb-7-2000-mafiaboys-moment-2/, consulted on 1.10.2023.

(1985), or Austria (1993), Romania (1996), Luxembourg (1997).

4. The fourth "wave" of reforms concerns the regulation of the distribution of illegal or harmful information, and was greatly boosted in the late 1980s by the growth of the Internet.

5. The fifth "wave" relates to changes in procedural law, with regard to the aspects of criminal procedure raised by the impact of information technology.

6. While the sixth 'wave' concerns the imposition of obligations and limits in the area of IT security.

Cybercrime is an active, constant and growing phenomenon of our times, frequently reflected in the media. One study even indicates that the fear of cyber-attacks exceeds that of ordinary theft or fraud.

The first cases of cybercrime were committed even before the advent of the internet and involved data theft. Computers, computer networks and the internet were created to create, store and transfer government and corporate information, information that is very valuable to the right people. The creation of digitized methods may have pushed humanity into the 21st century, but it has done the same for criminals. They want what we have and the harder it is for them to find, retrieve and use, the more they will want to take it. If not for personal gain, then just because they can.

Cybercrime really started to be discovered in the early 2000s, when social networking came to life. The rise of people putting all the information they could into a profile database created a flood of personal information and an increase in identity theft. Thieves used the information in a variety of ways, including accessing bank accounts, creating credit cards or other financial fraud.

Only a small proportion of criminal offences related to the use of information systems come to the attention of criminal investigation authorities, so it is very difficult to get an overview of the extent and development of the phenomenon. While it is possible to give an adequate description of the types of criminal offences encountered, it is very difficult to give an informed summary of the extent of the losses caused by these offences and the actual number of offences committed. The number of cases of cybercrime is constantly increasing. In Germany, for example, 32,128 such cases were recorded in 1996, in the Netherlands between 1981 and 1992 there were 1,400 cases, and in Japan between 1971 and 1995 there were 6,671 cases. It has been estimated that only 5% of the crimes committed come to the attention of the prosecution authorities.

To counter this lack of information, the survey process was used. The latest survey conducted by the Computer Crime Institute and the Federal Bureau of Investigation (FBI) in 2003 indicates losses of $201,797,340 for 538 US businesses and institutions surveyed.

During 2003, the specialised services in Romania investigated only 200 computer-related crimes, of which 50% were fraudulent electronic auctions, 30% fraudulently ordered goods online, 10% concerned unauthorised access to computer systems and 10% concerned Nigerian letters, transmission of viruses, child

pornography, use of false identities.

The increasing number of cybercrimes is driven by several causes, including:

- lack of specific training for prosecution officers;
- lack of a response plan in case of attacks by the victims of these criminal acts, which can lead to the losses caused not being identified;
- the delays in reporting crimes to criminal investigation authorities.

In the latter situation, even if the crime has been reported, the victims do not notify the prosecution authorities with a view to discovering and punishing the offender. There are many reasons for this behaviour. These include concerns about public image, which could be affected by the publicity surrounding the crime; the desire not to incur the costs of a possible investigation, given the complexity of such an investigation; and, last but not least, the lack of possibility of recovering the losses suffered, even if the offender is identified.

At the same time, cybercrime investigations are, by their nature, complex and involve the use of sophisticated, high-cost equipment. The training of specialist staff is also a lengthy and costly process. Such investigations are time-consuming. A cybercrime investigator can work on a maximum of 3-4 cases per month, whereas a traditional investigator can solve between 40 and 50 cases in the same period of time.

To this end, at international level, the Council of Europe has initiated a series of regulations on cybercrime. In 1995, Recommendation No. R (95) 13 was adopted on criminal procedural problems related to information technologies, and on 23 November 2001 the Convention on Cybercrime was signed in Budapest.

The Convention aims to prevent acts against the confidentiality, integrity and availability of information systems, networks and data, as well as the fraudulent use of such systems, networks and data, by ensuring that such conduct is criminalised and by encouraging the adoption of measures to enable such offences to be combated effectively, facilitating their detection, investigation and prosecution at both national and international level, and by providing for the necessary material provisions to ensure swift and secure international cooperation. The Convention was ratified by Romania through Law 64/2004 for the ratification of the Council of Europe Convention on Cybercrime, adopted in Budapest on 23 November 2001.

Statistics and reports from various sources support these findings. For example, the FBI's Internet Crime Complaint Center (IC3) reported a total of 791,790 complaints of alleged internet crime in 2020, with reported losses exceeding $4.2 billion. Of these complaints, the top three types of crimes reported were phishing scams, non-payment/non-delivery scams, and extortion. Similarly, a report by cybersecurity firm McAfee found that publicly disclosed cyber incident incidents increased 100% in the first quarter of 2020 compared to the same period the previous year.

3. Typology of cybercrime

Classification is a natural tool for the knowledge of objective reality, a special source of knowledge of it, a technique by which the set of observed phenomena is divided into main groups, classes, types that are part of a common system and constitute a single whole. In the classification process, each object studied is given a certain grade (rating). This is why, sooner or later, researchers are faced with the need to classify certain phenomena of social life. The content of the notion of computer-related crime, as mentioned in the previous content unit, is particularly varied, the approach to which differs from the perspectives of doctrinal views. For these reasons, the classification (typology) of these offences is also different.

Thus, in the report of the European Committee on Crime Problems, cybercrime is systematised into the following categories[16]:

- a computer fraud offence;
- the offence of computer forgery;
- the offence of damaging computer data or software;
- the offence of computer sabotage;
- the offence of unauthorised access to a computer;
- the offence of unauthorised interception;
- the offence of unauthorised reproduction of a computer program protected by law;
- the offence of unauthorised reproduction of a topography;
- the offence of unlawful alteration of data or computer programs;
- the offence of computer espionage;
- the offence of unauthorised use of a computer;
- the offence of unauthorised use of a computer program protected by law.

The United Nations Handbook for the Prevention and Control of Cybercrime summarises the following categories of crime[17]:

- computer fraud;
- fraud by falsification of documents;
- altering or modifying data or software;
- unauthorised access to information systems and services;
- unauthorised reproduction of legally protected software.

The study "Legal Aspects of Cybercrime in the Information Society" (COMCRIM study), carried out for the European Commission by Prof. Dr. Ulrich Sieber, University of Wurzburg, Germany, presents the following categories and sub-categories of cybercrime:

---

[16] Introductory guide to the application of legal provisions on cybercrime / Ministry of Communications and Information Technology. Bucharest, 2004, p. 51-52

[17] Sfetcu N., *Beginner's Guide for Cybercrime Investigators*, MultiMedia Publishing, ISBN: 978-606-033-093-6, 2014, p. 57.

1. interference with the right to privacy;

2. economic crimes:

- penetration of computer systems in order to overcome technical security difficulties ("hacking");
- computer espionage;
- software piracy;
- computer sabotage;
- computer fraud;
- distribution of illegal or harmful information (racist propaganda, dissemination of pornographic material, etc.);

3. other crimes:

- crimes against life;
- offences related to organised crime;
- electronic warfare.

In the Romanian doctrine some authors[18] distinguish the categories of cybercrimes according to the provisions of the Special Criminal Law no.161/ 2003 [19] as follows:

1. offences against confidentiality and integrity of data and information systems:

- the offence of unlawful interception of a computer transmission;
- the offence of altering the integrity of computer data;
- the offence of disrupting the functioning of information systems;
- the offence of carrying out illegal operations with computer devices or software.

2. cybercrime:

- the crime of computer forgery;
- the offence of computer fraud.

3. child pornography via computer systems.

Other researchers use the criterion of the role played by computer systems in the commission of the crime to classify computer crime. From this perspective, computer crimes are classified into:

- crimes committed with the help of information systems, where information systems are a tool to facilitate the commission of crimes. These are "traditional" crimes enhanced through the use of IT systems;
- offences committed by means of computer systems, where computer systems, including the data stored in them, are the target of the offence. These crimes can only be committed through computer systems. They have been the

[18] Florescu, V., Florescu G., *Analysis of computer crimes criminalized in the current legislation and in the perspective of the new penal cod*e, in: Romanian Journal of Informatics and Automatics, vol. 22, no. 2, 2012, p. 24.

[19] Romanian Law on some measures to ensure transparency in the exercise of public office, public functions and in the business environment, prevention and sanctioning of corruption, no.161 of 19 April 2003, Title III. In: Official Gazette of Romania, no. 279 of 21 April 2003.

subject of regulation in recent years.[20]

Depending on the perpetrator's attitude towards the crime committed, the motive that prompts him, we mention the following classification:

a) for selfish reasons: committed out of revenge; material interest; committed with heinous intent; terrorism.

b) unintentionally: committed out of curiosity; for self-affirmation purposes[21].

We also cannot ignore the typology of computer-related offences stipulated in the Council of Europe Convention on Cybercrime, adopted in Budapest on 23 November 2001[22], namely:

- offences against the confidentiality, integrity and availability of a computer system or electronic data: illegal access; illegal interception; alteration of data; unauthorised access to a computer system; use of unlawful methods.
- computer systems offences: computer systems forgery; computer systems fraud.
- electronic data content offences: child pornography offences.
- offences related to infringement of intellectual property and related rights.

Finally, making a retrospective of the classifications described above and by correlation with the provisions of the Criminal Code of the Republic of Moldova, we can establish two types of computer crimes:

- offences against confidentiality and integrity of data and information systems (provided in Articles 259, 260, 260^1-260^4, 261 of the Criminal Code of the Republic of Moldova);
- computer offences in the strict sense of the term (provided in Articles 260^5 and 260^6 of the Criminal Code of the Republic of Moldova)).

[20] Sfetcu, N., *op.cit*., p. 57; Grigoriev A.N., Meshkov V.M., Protsenko N.Yu., *Computer crimes and computer information protection. Scientific and practical manual*, Kaliningr Publishing House. Judicial Institute of the Ministry of Internal Affairs of Russia, Kaliningrad, 2003.

[21] Krilov, V.V., *op. cit*., p. 62.

[22] Council of Europe Convention on Cybercrime, adopted in Budapest on 23 November 2001, ratified by the Law on Ratification of the Council of Europe Convention on Cybercrime, adopted by the Parliament of the Republic of Moldova on 02.02.2009. In: Official Monitor of the Republic of Moldova, 2009, no. 37-40.

Chapter II.
Practical Aspects of Cybercrime in the Modern and Contemporary Criminal Law System

1. Harmonisation of cybercrime legislation worldwide

Harmonisation of cybercrime legislation worldwide is an important challenge for the international community. Currently, national cybercrime laws vary widely between countries and this discrepancy can lead to difficulties in investigating transnational cybercrime.

One way to harmonise legislation is through the adoption of an international convention on cybercrime. The Council of Europe Convention on Cybercrime (the Budapest Convention) is an example of such a convention that has been signed and ratified by a large number of countries around the world.

This convention harmonises definitions and penalties for a range of cybercrimes, including unauthorised access to a computer system, unauthorised interception of computer communications and intentional destruction or damage to computer data.

The challenges outlined at international meetings on combating cybercrime are very different, such as : lack of unanimous consensus on the content of the notion of "cybercrime" and the concept of "computer crime"; the motivation for committing these crimes; the expertise of authorised persons from institutions with supervisory powers in this field; the lack of an adequate legal platform for accessing and investigating information systems, including the absence of permissive provisions on the seizure of computer databases; unification of the legislative basis for investigations in this field, the transnational nature of this type of crime; the low number of international treaties on extradition and mutual assistance in this field.

Among the first international organisations to study the unification of legislation in this field was the Organisation for Economic Cooperation and Development (OECD), set up in 1947 to administer Canadian and American financial resources for the reconstruction of Europe after the Second World War and included in the Marshall Plan. It was renamed the OECD in 1961 with a different purpose - to assist member states in achieving sustainable economic development and raising living standards while maintaining financial stability. It currently lists some 30 member states and over 70 partner states). In 1983, the OECD produced a report in which it made a number of legislative recommendations to the EU Member States, as well as a minimum list of activities to be penalised: computer fraud and forgery, alteration of computer programs and data, copyright, interception of communications or other functions of a computer, unauthorised access and use of a computer.

At the same time, following the OECD's actions, the Council of Europe initiated a new case study to examine the legal framework for combating cybercrime with a view to its further development.

It is worth noting that the Council of Europe initiated elements of cybercrime at the 12th Conference of Directors of Criminological Research Institutes - Council of Europe Conference on the Criminological Aspects of Economic Crime (15-17 November 1976). In this context, a number of cybercrime offences were introduced, including for the first time the offence of fraud.[23]

Other activities indirectly related to the object of the study followed, such as the signing of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data in Strasbourg on 28 January 1981 (ratified by the Republic of Moldova by Decision of the Parliament of the Republic of Moldova No. 483-XIV of 2 July 1999).[24]

Since April 1976, several resolutions and recommendations have been adopted within the European Union (1976, 1979, 1982), culminating in the recommendation from the European Commission for Member States to sign the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, mentioned above.

The work of the European Commission and the Council of Europe has been immense, with several landmark events including the Luxembourg Conference (1987).

This was followed by the European Directive 91/250/EEC23 on the legal protection of computer programs, by which the European Union made it compulsory to respect copyright in this field and to punish computer piracy, and by Directive 95/46/EC24 on the protection of individuals with regard to automatic processing of personal data and on the free movement of such data, Member States were obliged to implement its provisions, which included the confidentiality and security of the processing of such data, as well as judicial remedies, sanctions and penalties.

The European legislator in April 1997 adopted a resolution on strengthening measures to combat harmful or illegal communications on the Internet, with particular reference to racist and pornographic material.

These recommendations were the prerequisites for the adoption of a European Convention - a legally binding instrument that can help to develop and/or standardise national legislation to combat cybercrime.[25]

---

[23] Stein Schonberg, *Computer-related crime*, Conference "Challenges of Cybercrime", Council of Europe, Strasbourg, 15-17 September 2004, available at http://www.cybercrimelaw.net/documents, consulted on 1.10.2023.

[24] By Act of the Parliament of the Republic of Moldova No. 271 of 07.11.2013, declarations of the Republic of Moldova to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data were formulated with regard to Art. 3 point 2 letters a), c); Art. 13 point 2 letter a).

[25] Spânu-Dumneanu, Ludmila, *International and national developments in the field of cybercrime*, https://juridicemoldova.md/6687/evoluarile-internationale-si-nationale-in-domeniul-infractiunilor

The international community in its large part recognizes that the Council of Europe Convention on Cybercrime is the economic part among the international legal regulations in the field of preventing and combating cybercrime, as it aspires to become that global legal instrument, being ratified and signed by a growing number of states from different parts of the world, signed in Budapest on 23 November 2001 (ratified by the Republic of Moldova by the Law of the Parliament of the Republic of Moldova No. 6 of 02.02.2009).

This international instrument aims to warn of actions directed against the integrity and availability of information systems, data confidentiality, networks and the illegal application of such acts and by encouraging the adoption of effective measures to combat computer-related crime, designed to facilitate their detection, investigation and prosecution both nationally and internationally, and by adopting provisions capable of ensuring international cooperation in a timely and useful manner.

The Council of Europe Convention on Cybercrime, also known as the Budapest Convention, was signed on 23 November 2001 and entered into force on 1 July 2004. To date, the Convention has been signed and ratified by the following countries: Albania, Andorra, Armenia, Austria, Azerbaijan, Belgium, Bosnia and Herzegovina, Bulgaria, Canada, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Georgia, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Mexico, Montenegro, Netherlands, New Zealand, Norway, Poland, Portugal, Romania, Russia, San Marino, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey, Ukraine, United Kingdom and United States of America.

There are also other countries that have signed but not yet ratified the Convention. The Convention mainly seeks to harmonise substantive criminal law provisions in the field of computer-related crime, to implement procedural provisions necessary for the investigation and prosecution of such offences and to establish a rapid and effective system of international cooperation.

While the first chapter of the Convention gives the meaning of certain terms and expressions, the second chapter deals both with the criminalisation of certain acts as offences and with other aspects of substantive criminal law relating to criminal liability, participation and sanctions.

Nine offences are defined, grouped into four different categories. Thus, the following offences are considered as offences affecting the confidentiality, integrity and availability of data and information systems: illegal access (Article 2), illegal interception (Article 3), alteration of data integrity (Article 4), alteration of system integrity (Article 5) and abuse of devices (Article 6). Computer-related offences are computer-related forgery (Article 7) and computer-related fraud (Article 8). Another category of offences concerns child pornography (Art. 9) and the last category concerns offences infringing intellectual property and

-informatice-lsd.html, consulted on 1.10.2023.

related rights (Art. 10).

Section II of Chapter II deals with procedural provisions in criminal matters applicable to the commission of the offences indicated, to the commission of any ordinary criminal offence by means of computer systems or where evidence of the commission of any offence is stored in a computer system. The conditions and protection measures are also laid down. Thus, measures are put in place on the expeditious preservation of stored computer data (Article 16), on the expeditious preservation and partial disclosure of traffic data (Article 17), on the order to make data available (Article 18), on the search and seizure of stored computer data (Article 19), on the real-time collection of traffic data (Article 20) and on the interception of content data (Article 21). Provisions on jurisdiction are also laid down. Chapter III contains provisions on international mutual legal assistance in criminal matters relating to computer-related crime, including provisions on extradition. It also lays the foundations for a 24-hour cooperation network between the signatory States in order to receive and deal promptly with requests for mutual legal assistance.

The commission of the offences described above requires, including in terms of information technology, specific modes of operation for each cybercrime. The biggest challenge is the difficulty in establishing the perpetrator, the scale and impact of the crime. Deficiencies in criminal procedural regulations in this area and the lack of knowledge of modern information technologies among prosecution officers facilitate high levels of latency.

For the purposes of the Law on preventing and combating cybercrime No 20 of 3 February 2009, a computer system means any isolated device or set of interconnected or linked devices which provides or of which one or more elements provide, through the execution of a program, the automatic processing of data. Cybercrime usually targets computers, networks or other forms of information and communication technology (ICT). It includes, for example, the creation and spread of malware, hacking to steal sensitive data and denial of service (DoS) attacks aimed at causing financial and/or reputational damage.

Cyber-attacks and cybercrime are increasing in number and sophistication in all European countries. This trend is expected to continue to grow in the future, with 22.3 billion devices worldwide expected to be connected to the Internet of Things by 2024.

The EU plans to strengthen its measures to fight cybercrime, in particular by targeting cybercriminals offering online specialised criminal services.[26]

Main cyber threats in the EU. Responsible for the theft of more than 10 terabytes of data every month, ransomware attacks are one of the biggest cyber threats in the EU and phishing is currently the most common initial vector for such attacks. Distributed Denial of Service (DDoS) attacks are also among the most potent threats.

[26] *EU fight against organised crime*, https://www.consilium.europa.eu/ro/policies/eu-fight-against-crime/, consulted on 1.10.2023.

The annual cost of cybercrime to the global economy has been estimated at €5.5 trillion by the end of 2020, double than recorded in 2015.

In 2022, Russia's military aggression against Ukraine has reshaped the threat landscape in Europe. The conflict has mobilised many hacktivists and cyber criminals and numerous state-sponsored groups.

Cybercrime is now one of the EU's priorities in the fight against serious and organised crime as part of EMPACT 2022 - 2025.

Making children safer online. In May 2022, the European Commission proposed new legislation to combat child sexual abuse and sexual exploitation of children online. The new rules are currently being discussed in the Council.

In the meantime, the EU has adopted temporary rules, by way of derogation from Articles 5(1) and 6(1) of the ePrivacy Directive, to allow webmail and messaging service providers to continue to detect online child sexual abuse.

Justice and law enforcement. EU rules and policies also address other justice and law enforcement aspects of fighting cybercrime and crime in general, such as access to electronic evidence, encryption and data retention.

Access to electronic evidence. Criminals exploit digital technology to commit crimes and hide illicit activities. As a result, law enforcement and judicial authorities are increasingly relying on electronic evidence, such as texts, emails or messaging applications, in their investigations and prosecutions.

This is why the EU is working on new rules that will make it easier and faster to access electronic evidence across borders.

Boosting cyber diplomacy. The European Union and its Member States strongly promote an open, free, stable and secure cyberspace in which human rights, fundamental freedoms and the rule of law are fully respected for the purposes of social stability, economic growth, prosperity and the integrity of free and democratic societies.

The EU is investing a lot of effort to protect itself against cyber threats from third countries, in particular through a common diplomatic response called the "cyber diplomacy toolkit". This response includes diplomatic cooperation and dialogue, preventive measures against cyber attacks and sanctions.

The EU Cyber Security Strategy, adopted by the European Commission and the EEAS in December 2020, strengthens the EU's diplomatic response to cyber attacks.

To further facilitate cross-border access to electronic evidence in criminal proceedings, the EU:

1. is negotiating an agreement with the US - the country where most service providers are located;

2. is participating in the negotiations for the second additional protocol to the Budapest Convention.

Encryption. The EU is working actively with the technology industry to strike the right balance between ensuring the continued use of strong encryption technology and guaranteeing that law enforcement and judicial authorities can

exercise their powers under the same conditions as in the offline environment.

In December 2020, the Council adopted a resolution on encryption, highlighting the need for both security through encryption and security despite encryption.

Data retention. Today, in order to fight crime effectively, it is important that service providers keep certain data that can be disclosed under certain strict conditions for the purpose of fighting crime. However, data retention may violate individual fundamental rights, in particular the rights to privacy and to the protection of personal data.[27]

The Council adopted conclusions on the retention of electronic communications data for the purpose of fighting crime. The Council instructed the Commission to collect further information and organise specific consultations as part of a comprehensive study on possible solutions for data retention, including consideration of a future legislative initiative.

Sanctions against cyber attacks within the EU. In May 2019, the Council established a framework allowing the EU to impose targeted sanctions to deter and respond to cyber attacks that pose an external threat to the EU or its Member States.

Specifically, this framework allows the EU, for the first time, to impose sanctions on persons or entities that are responsible for cyber attacks or attempted cyber attacks, provide financial, technical or material support for such attacks, or are otherwise involved. Sanctions may also be imposed on other persons or entities associated with them.

Restrictive measures include:

- ban on travellers to the EU;
- freezing the assets of persons and entities.

First sanctions for cyber attacks imposed on 30 July 2020.

Back in 2014, the EC estimated the *following developments in cybercrime*:

- the number of offenders is growing. The threshold for entry into cybercrime activities has become very low. A whole underground economy has already developed, in which various types of criminal products and services are traded, including drugs, weapons, contract killings, theft of identification data for online payments and child abuse. Any type of cybercrime can be carried out even without technical skills: password cracking, hacking, tailored malware or DDoS attacks.

- demand is growing. The demand for and use of cybercrime services is expected to increase, leading to further growth in the development, testing and distribution of malware; the creation and installation of botnets; the theft and trading of identification data for online payments; and money laundering services.

[27] *Cyber security: how the EU is tackling cyber threats*, https://www.consilium.europa.eu/ro/policies/cybersecurity/, consulted on 1.10.2023.

- sophistication increases. More aggressive and resilient types of malware are expected to develop. These include ransomware with more advanced and complex encryption; more resilient botnets; malware targeting banks and more sophisticated Trojans to circumvent protection measures taken by financial institutions.

- globalisation is growing. Due to the rapid spread of internet connections, cybercrime originating from South-East Asia, Africa and South America will increase**.**

- inclusion of mobile devices. Malware development is expected to be directed towards mobile devices so that they can operate and be distributed via such devices.

- smarter distribution. New ways of distributing aggressive and resilient types of malware are expected to emerge in the coming years. There is also a growing trend of concern, namely live streaming of child abuse, where police cannot obtain evidence unless they intercept the transmission**.**

- increased need for money laundering. Criminals will look for easy ways to make profits and launder money. The scenario of targeting large numbers of citizens and small to medium-sized businesses for relatively small amounts is likely to continue. But the use of online shopping and online payment identifiers will also increase. Demand for virtual currency and other anonymous payment systems will continue to grow.

- targeting cloud services. Attacks targeting cloud services are becoming increasingly interesting for criminals. Criminals are increasingly expected to target these services for espionage, data theft and extortion.

Moreover, in 2017 the European Commission produced the Report to the European Parliament[28], the European Council and the Council: "Sixth progress report on achieving a real and effective security union" in which it was established that: cyber-attacks are increasing in intensity, volume and quality.[29] Cybercrime is international: victims, offenders and evidence are often located in different countries, under several jurisdictions. Member States have shown a particular interest in making cybercrime a priority, as demonstrated by the number of operational action plans put in place in the areas of cyber-attacks, online child sexual exploitation and payment card fraud.

There is also a view that the most common and well-known method of deception through electronic means is phishing, whereby a user of electronic financial services is misled into communicating confidential information to unauthorised persons. This information is then used to gain access to the victim's bank accounts, to withdraw money from these accounts or to pay for various services

[28] *Sixth progress report on achieving a real and effective security union*. European Commission, Brussels 24.04.2017, www.ipex.eu, consulted on 1.10.2023.

[29] *Online Organised Crime Threat Assessment* (IOCTA) 2016: https://www.europol.europa.eu/activitiesservices/main-reports/internet-organised-crime-threatassessment-iocta-2016, consulted on 1. 10.2023.

and products. The techniques and methods used by the criminals are very diverse.[30]

Cybercrime is a modern phenomenon with important repercussions in everyday social life. Computers have become a criminogenic factor, providing both an object - the information contained and processed by computer systems - and a tool for criminal behaviour. It offers a repertoire of techniques and strategies for committing crimes, but at the same time it also enriches the criminal sphere with new computer crimes.[31]

At the end of 1997, during the G8 Summit in Denver, the Ministers of Interior and Justice of the countries attending the meeting took note of the unprecedented increase in cybercrime and adopted a final document. The G8 representatives discussed the danger of this type of crime, which they classified into two main areas:

- cybercrime that targets computer networks and telecommunications systems for destruction, causing significant damage to both public authorities and private individuals;

- terrorist or organised crime organisations using the facilities of new technologies to commit particularly serious crimes.

The Communication presented at the end of the G8 Summit in 1997 contains 10 principles and guidelines for action to combat cybercrime, ideas which have been quoted in many Recommendations and Directives that have been adopted since 1998. These principles were:

- there should be no safe place for those who abuse information technology;

- investigations and punishments for such crimes must be coordinated with the support of all states, even if no harm is done;

- the law must explicitly combat every such crime;

- the law must protect the confidentiality, integrity and usefulness of computer databases, and punish unauthorised intrusion into computer systems;

- the law must allow for the defence and preservation of fast-access databases, which are the most vulnerable to outside attacks;

- the mutual assistance regime of states must allow for regular and as-needed information sharing in the event of cross-continental crimes;

- access to open electronic databases must be free, without the consent of the State on whose territory they are located;

- the legal regime on the sending and authentication of electronic data used in cyber investigations must be developed;

- the extension of a practical and secure telecommunications system must be combined with the implementation of means to detect and prevent abuse;

---

[30] Milodin D., Sbora C., *Non-security - a prerequisite for cybercrime*. Theoretical and applied economics. Volume XIX (2012), No. 4(569), p. 36.

[31] Lazari, C. *Some aspects of cyberterrorism*, in: Scientific and Practical Review of the Institute of International Relations of Moldova, no.1, 2016, p.150.

- work in this area should be coordinated by international institutions and forums specialising in the field of IT.

For its part, the Action Plan included the following guidelines:

- using its own computer network and accumulated knowledge in the field to ensure accurate and effective communication on crime cases occurring in global networks;
- to take the necessary steps to create a modern and effective legislative system to combat the phenomenon and make it available to Member States;
- reviewing Member States' national legislation and harmonising it with the criminal legislation needed to combat cybercrime;
- negotiation of new assistance and cooperation agreements;
- development of technological solutions to enable cross-border searches and remote investigations;
- developing procedures to obtain data of interest from telecommunications system operators;
- concerted efforts with industry to obtain the latest technologies that can be used to combat cybercrime
- providing assistance in the event of urgent requests through its entire technological system;
- encouraging international IT and telecoms organisations to raise standards and safeguards for the private sector;
- to achieve single standards for the transmission of electronic data used in official or private investigations.

The European Union strategy to combat cybercrime is based on the common document of all European institutions - 11632/98 CR1MORG 149 - which presents the structure of the areas of interest resulting from the work of international fora and organisations, namely:

- duties and responsibilities of network administrators;
- fight against child pornography on the Internet;
- types of actions that can be classified as cybercrime;
- creation of a legal framework for cross-border cooperation;
- creation of a technological support to implement and harmonise the legal framework in this area;
- development of a standard international legal framework for sanctions applied to this type of crime.

The European Committee on Crime Problems of the Council of Europe recommended the elaboration of an international document committing the signatory states to the obligation to criminalise offences committed through computer systems, as well as to procedural provisions and international legal assistance in this field. A committee of experts on cybercrime was therefore set up and elaborated the Council of Europe Convention on Cybercrime signed in Budapest

on 23 November 2001.[32]

The Convention mainly seeks to harmonise substantive criminal law provisions in the field of computer-related crime, to implement procedural provisions necessary for the investigation and prosecution of such offences and to establish a rapid and effective system of international cooperation.

The importance of preventing and combating cybercrime has been underlined by the European Union in the "Internal Security Strategy of the European Union: Towards a European Security Model", adopted by the Justice and Home Affairs Council at its meeting on 25-26 February 2010 and endorsed by the European Council on 25-26 March 2010, under the chapter "Common Threats". The problem of cybercrime, according to the Strategy, is seen as one of the challenges to EU internal security and "poses a global, technical, cross-border and anonymous threat to our information systems and therefore poses many additional challenges to law enforcement authorities"[33]. To meet these challenges, numerous tools have been developed to facilitate cooperation, the most relevant of which are: analysis of future situations and scenarios to anticipate threats, as well as an appropriate response in terms of planning, programming and consequence management. Effectiveness on the ground is expected to be provided by the work of agencies, institutions and bodies within the EU. To this end, specific EU agencies have been set up, including EUROPOL, whose main objectives are to collect and exchange information and facilitate cooperation between law enforcement authorities in their fight against organised crime and terrorism. Another specific EU agency is EUROJUST, which ensures coordination and enhances the efficiency of judicial authorities. Last but not least, another agency, FRONTEX, manages operational cooperation at external borders.

The meeting in Brussels on 10 February 2014 under the title: "European Cybercrime Centre - one year after its establishment" was quite an important event, where the question was raised, among others: How has the European Cybercrime Centre (EC3) contributed to the protection of European citizens and businesses since its launch in January 2013?[34]

2. Analysis of cybercrime in the Republic of Moldova: regulations and actions at national level

In the Republic of Moldova, at present the normative sources regulating

[32] Council of Europe Convention on Cybercrime, http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Convention%20and%20protocol/ETS%20185%20Romanian.pdf, consulted on 1.10.2023.

[33] General Secretariat of the European Council, *Internal Security Strategy of the European Union: Towards a European Security Model*, Luxembourg: Publications Office of the European Union, ISBN 978-92-824-2690-6, p. 7.

[34] European Council press release: *European Cybercrime Centre - one year on*. Brussels, 10 February 2014, http://europa.eu/rapid/press-release_IP-14-129_ro.htm, consulted on 1.10.2023.

the legal aspects of the activity in the field of the national information infrastructure, as an environment for the functioning of the national information system in general, are established within several branches of law. In addition to the field of criminal law provisions, other special normative acts are adopted and applied:

- Criminal Code of the Republic of Moldova, Chapter XI Cybercrimes and Telecommunications Offences;

- Law on Informatics, adopted by the Parliament of the Republic of Moldova on 22.06.2000[35];

- Law on Computerization and State Information Resources, adopted by the Parliament of the Republic of Moldova on 21.11.2003[36];

- Order of the Minister of Transport and Communications approving the National Telecommunications Strategy No. 18 of 23.01.2001[37];

- Telecommunications Development Strategy (Introduction), approved by Order of the Minister of Transport and Communications No. 188 of 11.11.2004[38];

- Government Decision no.857 of 31.10.2013 on the National Strategy for the Development of the Information Society "Digital Moldova 2020" [39], etc.

The regulation of cybercrime in the legislation of the Republic of Moldova came as a natural adaptation of the legislation to realities that could not be ignored. Thus, in the Criminal Code of the Republic of Moldova, adopted by Law No. 985 of 18.04.2002, in force since 12.06.2003, for the first time, the chapter "Computer offences and offences in the field of telecommunications", which originally contained three articles, was introduced:

1. Article 259 - Illegal access to computer information;

2. Article 260 - Illegal production, import, marketing or making available of technical means or program products

3. Article 261 - Breach of computer system security rules.

After the ratification of the Council of Europe Convention[40] on Cybercrime, adopted in Budapest on 23.11.2001, by Law No. 6 of 02.02.2009, the Criminal Code of the Republic of Moldova, being harmonized in accordance with the provisions of the Convention by Law No. 278 of 18.12.2008, both published

[35] Law No. 1069 of 22-06-2000 on informatics, Official Monitor of the Republic of Moldova, 2001, No.73-74.

[36] Law, No. 467 of 21-11-2003 on computerization and state information resources Official Gazette of the Republic of Moldova, 2004, No.6-12.

[37] Order No. 18 of 23-01-2001, Ministry of Transport and Communications, Official Monitor of the Republic of Moldova, 2001, No. 8.

[38] Telecommunications Development Strategy, Official Monitor of the Republic of Moldova, 2004, no. 218-223, art. 460.

[39] National strategy for the development of the information society "Digital Moldova 202", Official Monitor of the Republic of Moldova, 2013, no.252-257

[40] Recommendation for a Council Decision authorising participation in negotiations on the Second Additional Protocol to the Council of Europe Convention on Cybercrime (CETS No. 185), https://eur-lex.europa.eu/legal-content/RO/ALL/?uri=CELEX:52019PC0071, consulted on 1.10.2023.

in the Official Monitor on 20.02.2009, was supplemented with new articles 260^1 – 260^6, which provided for new types of offences, such as illegal interception of data transmission, disruption of the functioning of the computer system, computer forgery, computer fraud, etc.[41]

Currently, the Criminal Code of the Republic of Moldova provides for the following cybercrimes:

- Article 259. *Illegal access to computer information*;
- Article 260. *Illegal production, import, sale or making available of technical means or program products*.
- Article 260^1. *Illegal interception of a computer data transmission.*
- Article 260^2. *Altering the integrity of computer data held in a computer system*.
- Article 260^3. *Disruption of the functioning of the computer system*.
- Article 260^4. *Illegally producing, importing, trading or making available passwords, access codes or similar data.*
- Article 260^5. *Computer forgery*.
- Article 260^6. *Computer fraud.*
- Article 261. *Breach of computer system security rules.*
- Article 261^1. *Unauthorised access to telecommunications networks and services.*

2.1. Characteristics of computer-related crime in the Republic of Moldova

The computer-related offences set out in Chapter XI "Computer-related and telecommunications offences" are much more complex than may be apparent at first glance. Against this background, the following is a generalisation of their common and distinct features.

As the features of the offences are characterised by the objective and subjective elements of their composition, the research is based on determining them.

The generic legal object of computer-related offences derives from the group of offences included in Chapter XI referred to above, which is expressed as social values and social relations in the field of information technology and telecommunications.

Determining the special legal object of computer-related offences, we establish that the offences provided for in Article 259 of the Criminal Code of the Republic of Moldova have a complex special legal object which is composed of: the main legal object consisting of social relations regarding legal access to computer information; and the secondary legal object represented by social relations

[41] Criminal Code of the Republic of Moldova, No. 985-XV of 18.04.2002. In: Official Monitor of the Republic of Moldova No. 128-129/1012 of 13.09.2002, republished in: Official Monitor of the Republic of Moldova No. 72-74/195 of 14.04.2009.

regarding legal intervention in the information system.

In the case of the offences referred to in Articles 260-261 of the Criminal Code of the Republic of Moldova, there is a simple special legal object consisting of social relations with regard to:

- legal circulation of technical means or programmed products (art. 260 Criminal Code of the Republic of Moldova);
- the legality of interception of a transmission of computer data that are not public (art. 260^1 Criminal Code of the Republic of Moldova);
- integrity, accessibility and legal circulation of computer data (art. 260^2 Criminal Code of the Republic of Moldova);
- the proper functioning of a computer system in terms of the inviolability of the computer domicile (art. 260^3 Criminal Code of the Republic of Moldova);
- reliance on computer data allowing access to a computer system, for the purpose of their correct and lawful use, as well as the correct and lawful conduct of business operations in relation to them (art. 260^4 Criminal Code of the Republic of Moldova);
- public confidence in the safety and reliability of information systems, in the validity and authenticity of computer data, of the entire modern process of automatic processing, storage and transaction of data of official or private interest (art. 260^5 Criminal Code of the Republic of Moldova);
- the integrity of a person's assets, when the presence of that person in cyberspace is quantified in a certain volume of data stored in a computer system or circulated in a network (art. 260^6 Criminal Code of the Republic of Moldova);
- security of the computer system (art.261 Criminal Code of the Republic of Moldova).

In the context of computer-related crimes as a material or immaterial object of the crime is presented:

- computer information, computers, computer system or computer network (Article 259 of the Criminal Code of the Republic of Moldova);
- information protected by law (letter g) paragraph. (2) art. 259 Criminal Code of the Republic of Moldova);
- technical means or program products, designed or adapted, for the purpose of committing one of the offences referred to in Articles 237, 259, 260^1-260^3, 260^5 or 260^6 of the Criminal Code of the Republic of Moldova (Article 260 of the Criminal Code of the Republic of Moldova);
- transmission of computer data (including an electronic transmission) which is not public and which is intended for a computer system, if it originates from such a system or is carried out within a computer system (art. 260^1 Criminal Code of the Republic of Moldova);
- computer data from a computer system, from a storage medium or with limited access (Art. 260^2 Criminal Code of the Republic of Moldova);
- computer data (Art. 260^3, 260^5 and 260^6 Criminal Code of the Republic of Moldova);

- passwords, access codes or similar data allowing full or partial access to a computer system (art. 260^4 Criminal Code of the Republic of Moldova);

- computer information or other entities, inherent in the background of causing serious consequences (art.261 Criminal Code of the Republic of Moldova).

In this context, we mention that computer data that are not true are the product of the crime criminalized in Article 2605 Criminal Code of the Republic of Moldova.

As victims of the crimes under investigation are persons with the following characteristics:

- owner or other possessor of the computer information, computer, computer system or computer network illegally accessed (art.259 Criminal Code of the Republic of Moldova);

- natural or legal person, owner of technical means or program products that have been fraudulently used to allow access to a computer system (art.260 Criminal Code of the Republic of Moldova);

- natural or legal person who is the owner of the intercepted computer data (art. 260^1 Criminal Code of the Republic of Moldova);

- natural or legal person in possession of the computer data which constitutes the immaterial object of the offence (art. 260^2 Criminal Code of the Republic of Moldova);

- natural or legal person in possession of the computer system, the functioning of which is disturbed (art. 260^3 Criminal Code of the Republic of Moldova);

- natural or legal person in possession of passwords, access codes or other such computer data which have been fraudulently used to allow access to a computer system (art. 260^4 Criminal Code of the Republic of Moldova);

- natural or legal person whose interests have been damaged and who suffers legal consequences (financial, moral or social) as a result of the counterfeiting of computer data (Article 260^5 of the Criminal Code of the Republic of Moldova);

- a person whose property interest has been damaged by the perpetrator's action (Article 260^6 of the Criminal Code of the Republic of Moldova);

- owner or other possessor of information resources or systems, technologies and means of securing them; owner or other possessor of computerised information (Article 261 of the Criminal Code of the Republic of Moldova).

As mentioned in the literature, the objective side of computer crimes[42], is characterized by the fact that the harmful act can be committed by action (art. 259, 260, 260^1 – 260^6 of the Criminal Code) or by action or inaction (art. 261 of the Criminal Code). From the point of view of the structure of the objective side,

[42] Branza, N., State, V., *Treatise on Criminal Law. Special Part*, volume II. Chisinau: Tipografia centrala, 2015, p. 344.

the offences in question are material offences (in the case of the offences specified in Articles 259, 260^2 – 260^6, 261 CC RM) or formal offences (in the case of the offences specified in Articles 260 and 260^1 Criminal Code of the Republic of Moldova).

In the context of computer-related offences, the following means of committing the offence become mandatory as an optional sign of the objective side of the offence:

- special technical means (letter e) paragraph (2) art.259 and letter d) paragraph (2) art. 261^1 Criminal Code of the Republic of Moldova);

- computer, computer system or computer network letter. (f) paragraph (2) art. 259 Criminal Code of the Republic of Moldova).

As regards the subjective side of computer-related offences, although the rules in Chapter XI "Computer-related and telecommunications offences" of the Special Part of the Criminal Code do not specify the form of guilt, it is characterised by:

- intention (art. 259, 260, 260^1 – 260^6 Criminal Code of the Republic of Moldova);

- intent or recklessness in relation to the harmful act and only recklessness in relation to the harmful consequences (art. 261 Criminal Code of the Republic of Moldova).

When committing the offences referred to letter f) paragraph (2) art. 259, art. 260, 260^4 – 260^6 Criminal Code of the Republic of Moldova the legislator establishes as a mandatory sign the special purpose, namely:

- the purpose of committing one of the offences specified in paragraph (1) of Article 259, Articles 260^1-260^3, 2605 and 260^6 of the Criminal Code of the Republic of Moldova (letter f) paragraph (2) of Article 259 of the Criminal Code of the Republic of Moldova);

- for the purpose of committing one of the offences specified in Art.237, 259, 260^1-260^3, 260^5 and 260^6 Criminal Code of the Republic of Moldova (Art. 260 and Art. 2604 Criminal Code of the Republic of Moldova);

- the purpose of using untruthful data to produce a legal consequence (in Art. 260^5 Criminal Code of the Republic of Moldova);

- the purpose of obtaining a material benefit (art. 260^6 Criminal Code of the Republic of Moldova).

Also, the motive as a secondary sign of the subjective side of the offence, which is expressed in the interest of the matter, becomes obligatory in the case of the acts criminalized in letter a) paragraph (2) art. 260^3 and letter a) paragraph (2) art. 260^4 Criminal Code of the Republic of Moldova.

Finally, we distinguish that the subject of computer-related offences may be a responsible natural person who at the time of the commission of the offence has reached the age of 16 years (Art. 259, 260^1 – 260^6, 261 Criminal Code of the Republic of Moldova) or 14 years (Art. 260 Criminal Code of the Republic of Moldova). Also, the subject of the offences under Articles 259, 260, 260^1, 260^3,

260[4], 261 of the Criminal Code of the Republic of Moldova may be a legal person.

With reference to the subject of offences under Article 259 of the Criminal Code of the Republic of Moldova, he or she has a special status, namely a person who is not authorised by law or contract and who exceeds the limits of authorisation or does not have permission from the competent person to use, administer or control a computer system or to conduct scientific research or carry out any other operation on a computer system. Also, the person whose obligations include compliance with the rules of collection, processing, storage, dissemination, distribution of information or the rules of protection of the computer system is the special subject of the offence provided for in Article 261 of the Criminal Code of the Republic of Moldova.

Digital technology is frequently exploited to commit crimes and hide illicit activities. As a result, law enforcement and judicial authorities are increasingly relying in their investigations and prosecutions on electronic evidence, such as texts, emails, IP addresses or messaging applications.

Every year, the National Police register more than 200 cyber and related crimes. These crimes include identity theft, bank card theft, hacking into personal accounts, blackmail or online assault. In the Republic of Moldova, the most vulnerable areas are social engineering (psychological manipulation to perform actions and/or disclose information), identity theft, fraud when making payments abroad, etc.

Online security measures and the prevention of cyber attacks are becoming increasingly important for every citizen today. Knowing how to protect yourself online is the first step towards securing your digital assets and your privacy.

The actions of the authorities responsible for preventing cybercrime are as follows:

- **public information campaigns.** In order to provide citizens with more information, the police officers of the Cybercrime Investigation Directorate (DIII) of the IGP's INI have focused their efforts on preventing cybercrime by informing the population about vulnerable areas, precautionary measures and where they can file a complaint. In October 2022, police officers carried out a nationwide information campaign entitled "Be cautious! Use payment cards safely". This campaign aimed to produce beneficial effects on cyber education among citizens and the cultivation of responsible and aware behaviour. Citizens learned how to secure their personal accounts effectively, what to do in the first instance if their identity has been stolen and where to turn for help.[43] Such actions are part of the measures taken by the MFA to increase security in the online environment, including by promoting and strengthening international cooperation, such as with Spain, the Czech Republic, Germany, France, Hungary, Austria, Ukraine and the United States, as well as with organisations such as Interpol and

[43] Informing citizens about cybercrime and how to protect personal data and assets, https://www.mai.gov.md/ro/node/7213, consulted on 1.10.2023.

Europol. Measures taken also include institutional development of DIII, improving legislation and promoting partnerships with business and civil society.

- aligning our country with the international legal framework on cyber security. A rather important moment to note is that in November 2022, the Republic of Moldova signed the second additional protocol to the Council of Europe Convention on Cybercrime (Budapest Convention), together with 5 other states such as Croatia, the United Kingdom, Slovenia, Ukraine and Sri Lanka.[44] This protocol will improve cross-border access to electronic evidence for use in criminal proceedings. This will contribute to the fight against cybercrime and other forms of crime worldwide by simplifying cooperation between Member States and third countries, while ensuring a high level of protection for individuals and compliance with EU standards. A new guide, a guidance note on ransomware crime, was adopted at the meeting. The guide shows how the provisions of the Convention on Cybercrime and the new Additional Protocol can be used to criminalise, investigate and prosecute ransomware-related crimes.

Ransomware is malicious software that, once installed on a victim's device (computer, smartphone), encrypts the victim's data and blackmails the victim into publishing their data or simply not decrypting their data unless they pay a ransom.

In April 2023, employees of the Cybercrime Investigation Directorate, participated in the 9th Virtual Currencies Conference organised by Europol in the Hague, where they discussed the development of cryptocurrencies and their involvement in cybercrime, including ransomware attacks and illegal transactions.

Even though investigating cybercrime and other cross-border crimes involving cryptocurrencies can be difficult, as they are often used anonymously and without trace, all law enforcement authorities are constantly struggling to combat these illegal activities. Blockchain and cryptocurrencies can also be used in a positive way to combat money laundering and terrorist financing. Blockchain technology can be used to create a transparent and secure record of transactions, which can be accessed by law enforcement authorities if there is suspicion of illegal activity, and is very important for the Republic of Moldova and its future, for a proper analysis of financial transactions.

On 28 April, the General Inspectorate of Police informed citizens that a new type of message with false content, using the names of public authorities, is being distributed on e-mail addresses. Cyber criminals are sending fake summonses using the victims' e-mail addresses and, under the pretext that the authority in question has compromising images with sexual overtones, are asking the recipients to provide additional information and subsequently financial means.

In this context, citizens are urged to be vigilant and verify any information received. Police remind citizens that they can be victims of several types

[44] Better access to electronic evidence to fight cybercrime and related crimes, https://www.mai.gov.md/ro/node/7359, consulted on 1.10.2023.

of scams:

- staging a car accident and calling relatives of the alleged person involved in the accident, and then asking for a large sum of money.
- phone calls from a purported banking institution asking for bank card details and withdrawing money.
- cyber scam operated by hacking into the victim's personal profile and asking for money from virtual friends.

2.2. Actions to be taken in the Republic of Moldova to minimise cybercrime

In the Police Activity Report for 2022 it is shown that in this period, for the commission of cybercrimes and crimes in the field of electronic communications, 206 criminal cases were initiated, compared to 221 criminal cases registered in the analogous period of 2021.

The number of offences committed with the use of information systems by fraud registered 78 cases, has experienced an upward dynamic compared to the analogous period of last year where 16 cases were registered.

If we refer to the evolution in the last years, especially the crime of computer fraud (art. 260^6 of the Criminal Code of the Republic of Moldova), this year there is a decrease with 5 criminal cases registered compared to 7 criminal cases registered in 2021.

In order to redress the situation, it is necessary to provide modern equipment and tools, to harmonise the regulatory framework regulating the phenomenon of cybercrime, including the media and raising awareness of society about computer-related and related crimes committed through the use of information systems and modern technical means.

In order to raise public awareness of the phenomenon of cybercrime, during 12 months of 2022, the Cybercrime Investigations Directorate has published 16 press releases, conducted 9 interviews, 5 participations in broadcasts and 2 lessons to inform the public about methods of protection against different types of fraud.[45]

In the Programme for Preventing and Combating Crime for the years 2022 - 2025[46], in the area of preventing cybercrime and increasing cyber security, the following are proposed to be achieved:

- to step up efforts to fight cybercrime, including by creating a comprehensive legal and institutional framework in line with the Budapest Convention;
- engage, together with EU partner institutions, in professional capacity building and technical capacity building to fight cybercrime effectively;

[45] Police Activity Report 2022, https://politia.md/sites/default/files/raport_activitate_12_luni_2022_.pdf, consulted on 1.10.2023.

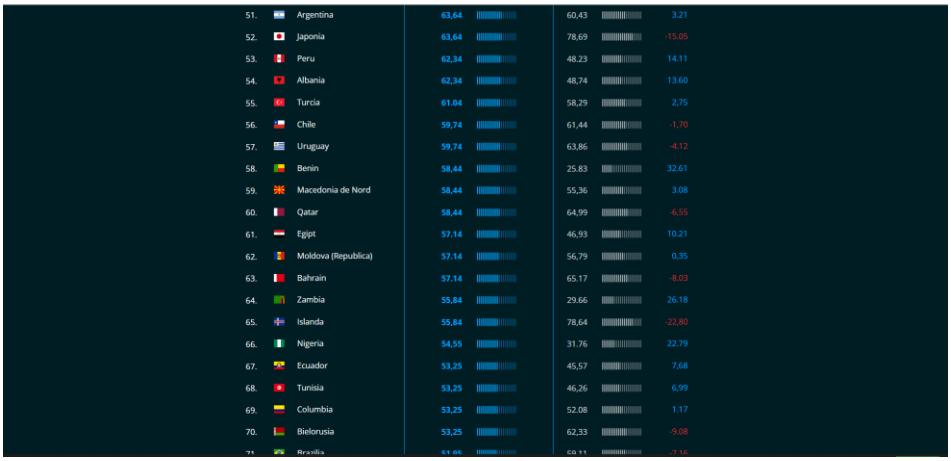
[46] Programme to prevent and combat crime for the years 2022 - 2025, https://cancelaria.gov.md/sites/default/files/document/attachments/721.pdf, consulted on 1.10.2023.

- ensuring the implementation of measures on the cyber security component of the Information Security Strategy of the Republic of Moldova for 2019-2024 and its Action Plan (HP No. 257/2018);

- strengthening cybersecurity by transposing into national legislation Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 on measures for a high common level of security of networks and information systems in the Union (NIS Directive);

- the identification and formal designation of a national CERT (Cyber Emergency Response Team), and the establishment of a clear division of labour and competences between agencies involved in ensuring cyber security, etc.

Fig. 2. Ranking of Moldova according to NCSI



Source: https://ncsi.ega.ee/ncsi-index/?order=rank&archive=1

By analysing the NCSI Index, it is possible to see the level of cyber security and maturity of each country worldwide. The NCSI is owned and developed by the Estonian e-Government Academy Foundation. It is an indicator used to assess a country's cybersecurity efforts and achievements. Thus, according to Fig. 2, it is possible to conclude that Belgium is the leader in cybersecurity. Moldova ranks 61st in this ranking with an index of 57.14, while Belgium has a score of 94.91. Moldova still has a lot of work to do to reach the top. It has backlogs and zero points on the indicator "Cyber security strategy implementation plan". It also has zero points for not having a cyber threat analysis unit.[47]

[47] National Cyber Security Index, https://ncsi.ega.ee/compare/, consulted on 1.10.2023.

3. Cyber criminals - sanctions imposed in the modern and contemporary legal system

The prosecution of cybercriminals often involves the collection and use of digital evidence, such as data from electronic devices or online traffic logs. Here are some examples of the types of digital evidence that can be used in criminal investigations of cybercrime:

- data from electronic devices: electronic devices such as mobile phones, tablets or computers may contain data relevant to investigations, such as emails, text messages, photos, videos, call logs or location data. This data can be used to establish the location of the offender, the time and manner of the cybercrime.

- online traffic logs: online service providers typically keep logs containing information about user activity, such as IP addresses, session information and activity on websites. These logs can be used to establish the identity of criminals, the type and amount of data stolen or how cybercrime was committed.

- financial data: financial data, such as bank transactions or online accounts, can be used to identify criminals and establish how they gained access to sensitive financial information or committed fraud.

- encrypted data: criminals may use encryption methods to protect their sensitive data or to hide their online activity. In such cases, investigators must use decryption methods or other investigative techniques to access relevant data.

- international practices on cyber investigations: cyber investigations are a major concern worldwide, as cybercrime is a global phenomenon that knows no borders. As a result, there are many international practices that would lead to faster identification of cyber criminals, including:

- *international collaboration:* governments and law enforcement organisations are increasingly collaborating internationally to investigate cybercrime. This can include sharing information and expertise as well as joint investigations. In addition, some international organisations, such as Interpol, have developed special programmes to help fight cybercrime.
- *standardisation of investigation practices:* efforts are underway to develop common standards and best practices for cyber investigations. These standards typically include procedures for collecting and storing digital evidence, as well as ways to collaborate with other organizations.
- *use of specialised technology:* although cybercriminals may use advanced technology to hide their tracks, there is also specialised technology that can be used in investigations. This can include data analysis software, encryption and decryption tools, and specialised equipment for collecting digital evidence.
- *improving investigative capacity:* governments and law enforcement organisations have increasingly invested in developing capacity to investigate cybercrime. This can include training of cyber investigation specialists and the creation of specialised cyber investigation laboratories and teams.

➢ *improved legislation:* Many countries have introduced or improved legislation to deal with cybercrime threats. This may include increasing penalties for cybercrime, as well as extending jurisdiction to allow offenders to be prosecuted and tried abroad.

Overall, international efforts to combat cybercrime are important because cybercrime can have a significant impact on economies and societies around the world.

3.1. Sanctions and punishment of cybercriminals in the modern criminal law system

It is important to note that cybercrime only started to be recognised as a major problem after the 1990s, with the increase in the use of computers and the internet. As a result, sanctions and penalties for computer crime in the modern legal system were limited and, in most cases, lacked specific laws dealing with such crimes.

In general, during this period, computer crimes were treated as ordinary theft or fraud offences, and penalties were determined by the seriousness of the offence and the damage caused. For example, an individual who stole information from a company could be charged with theft or industrial espionage and receive a penalty commensurate with the crime.

As cybercrime was not a significant problem in the modern legal system, the penalties and punishments for it were not widespread and did not exist specifically in the criminal codes of many countries. However, there are some notable examples of cybercrime in this time period, such as:

- in the 1980s, a new form of computer crime known as hacking developed. During this period, hacking became a popular activity among teenagers and young technology enthusiasts who wanted to explore the limits of computer systems. Although hacking was generally considered a misdemeanour during this period, some more serious cases led to higher penalties.

- in 1986, a German hacker was sentenced to 2 years in prison for illegally accessing US government and military computers.

- in 1988, Morris Worm, a computer program created by Robert Tappan Morris, infected several computer systems and caused more than $10 million in damage. Morris was sentenced to three years probation, a $10,000 fine and 400 hours of community service.

- in 1989, another German hacker was sentenced to 1 year in prison for illegally accessing NASA computer systems.

Because computer crime was not such a widespread problem between 1900 and 1990, punishments and sanctions for it were often limited to existing laws and rules in areas such as property theft, fraud and unauthorized computer access. However, as these laws and rules have continued to develop and adapt to the growing threat of cybercrime, as mentioned above, it has become increasingly

common for these crimes to be included in criminal codes and punishable by fines, imprisonment, or both.

In summary, in the modern criminal law system, sanctions and penalties for cybercrime have been determined according to existing laws and regulations, which did not specifically address cybercrime. However, with the increase in the use of computers and the internet, it has become increasingly important to develop specific laws and regulations to address this problem.

3.2. Sanctions for cybercrime in the contemporary legal system

In recent decades, sanctions and penalties for cybercriminals have developed considerably with the growth in computer and internet use and the emergence of increasingly complex and sophisticated threats. The following is a brief overview of sanctions and penalties for cyber criminals from 1990 to 2023.

Years 1990 - 2000: in the 1990^{s}, cybercrime laws and regulations were still developing. In general, sanctions and penalties were determined by the seriousness of the crime and the damage caused.

In 1995, Vladimir Levin, a Russian hacker, was arrested for stealing $10 million from Citibank through a computer network. He was extradited to the United States, where he was sentenced to thirteen years in prison and fined $240,015.

In 1996, the United States passed the Computer Fraud and Abuse Act, which provided a clear definition of and penalties for cybercrime.

Years 2000 - 2010: in the 2000^{s}, penalties and sanctions began to become more severe as cyber threats increased.

In 2002, the European Union adopted a Directive on the fight against cyber fraud, which introduced tougher penalties for cyber crime.

In 2003, the United States passed the CAN-SPAM Act, which established penalties for spam and phishing.

Years 2010 - 2020: in the 2010^{s}, sanctions and punishments continued to grow as internet and technology use increased.

In 2013, the European Union adopted a directive on preventing and combating cyber attacks, which introduced tougher penalties for cyber crime and encouraged international cooperation.

In 2015, the United States passed the Cybersecurity Information Sharing Act, which encouraged companies to share information about cyber threats and established penalties for cyber criminals.

Years 2020-2023: in recent years, sanctions and penalties for cybercrime have continued to grow and intensify as cyberthreats have increased.

In 2020, the European Union adopted a set of cyber security rules for digital services and set penalties for breaches.

In 2021, the United States adopted a new set of sanctions for foreign cybercriminals, including economic sanctions.

Penalties and sanctions for cybercrime vary widely in different countries and legal systems. Here are some of the penalties applied in different countries for cybercrime in the contemporary legal system:

- **U.S.A.**: the CFAA is the main federal law criminalising computer-related crimes. Penalties for computer crime can include fines, imprisonment or both. For example, unauthorised access to a protected computer can result in a fine and/or up to ten years in prison.

- **United Kingdom**: the Computer Misuse Act 1990 is the main legislation governing computer-related offences in the UK. Penalties for computer offences can include imprisonment and fines. For example, unauthorised access to computer material can lead to a fine and/or up to two years' imprisonment, while unauthorised access with intent to commit or facilitate other offences can lead to up to ten years' imprisonment.

- **Germany:** the German Criminal Code includes provisions criminalising computer-related offences such as unauthorised access and data interception. Penalties for computer crime can include imprisonment and fines. For example, unauthorised access to data stored in a computer system can lead to up to two years in prison.

- **Japan:** Unauthorised Computer Access Law criminalises unauthorised access to computer systems. Penalties for computer offences can include imprisonment and fines. For example, unauthorised access to a computer system can lead to up to three years in prison or a fine of up to 500,000 yen.

- **Australia**: Australia's Criminal Code Act 1995 includes provisions criminalising computer-related offences such as unauthorised access and data interception. Penalties for computer offences can include imprisonment and fines. For example, unauthorised access to restricted data can lead to up to two years in prison.

In general, penalties and sanctions for cybercrime are becoming increasingly severe as technology continues to play a more important role in our daily lives. It is important for individuals and organisations to be aware of the legal consequences of engaging in computer-related crime and to take steps to prevent such activities.

Here are some examples of **computer crime and the penalties applied, in the contemporary legal system**:

- in 1995, Vladimir Levin, a Russian hacker, was arrested for stealing $10 million from Citibank through a computer network. He was extradited to the United States, where he was sentenced to thirteen years in prison and fined $240,015;

- in 2000, a group of hackers called "Milw0rm" attacked several websites, including Microsoft's website. One of the group members, a Canadian teenager named Jonathon James, was caught and sentenced to 6 months in prison and a

$10,000 fine;

- in 2003, Adrian Lamo, an American hacker, was sentenced to 6 months house arrest and ordered to pay $65,000 in damages for unauthorised access to the computer network of The New York Times and other companies;

- in 2004, a German hacker named Sven Jaschan was sentenced to one year in prison suspended and ordered to perform community service for creating a computer virus called "Sasser" that infected millions of computers worldwide;

- in 2005, American hacker Kevin Mitnick was released from prison after a 5-year sentence for unauthorised access to the computer networks of several companies and government institutions. He was also ordered to spend three years under strict supervision after his release;

- in 2008, American hacker Albert Gonzalez was sentenced to 20 years in prison for stealing millions of credit card numbers through attacks on several companies' computer networks;

- in 2008, a Romanian hacker was sentenced to 21 months in prison for credit card fraud after compromising the credit card information of more than 1,000 people;

- in 2009, a Romanian hacker was sentenced to three years in prison and fined $240,015 for unauthorised access to NASA servers and making sensitive information public;

- in 2010, Australian hacker Julian Assange was charged with hacking into computer networks and was forced to live under house arrest for 10 months in the UK before being extradited to Sweden for questioning on the charges;

- in 2012, an Australian hacker was sentenced to 3 years in prison for identity theft and credit card fraud;

- also in 2012, two members of the LulzSec hacker group were sentenced to prison for unauthorised access to websites, including the Sony Pictures Entertainment website;

- in 2013, a New York hacker was sentenced to 10 years in prison for identity theft and unauthorized access to servers;

- in 2016, a Russian hacker was sentenced to 27 years in prison for email fraud, breaching computer systems and stealing personal information;

- in 2017, an Australian hacker was sentenced to 2 years in prison for unauthorized access to a telecommunications company's servers and obtaining customer information;

- in 2019, a British hacker was sentenced to 5 years in prison for unauthorised access to servers of government and corporate organisations;

- in 2021, an Australian hacker was sentenced to 2.5 years in prison for unauthorised access to a university's servers and stealing personal information of students and teachers;

- in 2021, a group of hackers from Russia was sanctioned by the U.S. Treasury Department on charges of conducting a series of cyberattacks against organizations and critical infrastructure in the United States;

- in 2019, the US government announced sanctions against the North Korean group Lazarus for its role in the attack on cryptocurrency exchanges. The sanctions included an asset freeze and a ban on any business with the group;

- in 2020, a group of Russian hackers who attacked US government networks and companies were sanctioned by the US Treasury Department, which imposed travel restrictions and froze their assets;

- in 2020, the European Union imposed sanctions against Russian, North Korean and Chinese intelligence services for their hacking and spying activities;

- in the UK, scientists working on the development of a vaccine for COVID-19 were the target of a cyber attack. The government has said that these criminals will be held accountable;

- in India, a group of hackers who targeted health and government systems during the pandemic have been arrested. These criminals have been charged with wire fraud and data theft;

- in Canada, a man who attacked websites providing information on COVID-19 was sentenced to 45 days in jail and fined C$2,000;

- in 2021, a Russian hacker was sentenced to 12 years in prison by a US court for his involvement in cyberattacks affecting companies, educational institutions and the US government. He was also ordered to pay a $19.2 million fine;

- in 2021, the European Union imposed sanctions against Russia for cyber attacks on the European Union and its member countries;

- in 2022, the U.S. Department of Justice sentenced a Russian hacker to 27 years in prison for his role in cyberattacks that affected several companies in the U.S. and other countries. He was also ordered to pay a $26.2 million fine.

These examples show that penalties for cybercrime in the 2000s and up to 2019, have continued to develop and become more specific, and offenders have started to receive harsher penalties for such crimes. In the years 2019 - 2023, sanctions for cybercrime have become increasingly severe and sophisticated, particularly after the emergence of the COVID-19 pandemic, and authorities in different countries have sought to take stronger action against cybercriminals.

Chapter III
Comparative Analysis of Cybercrime

1. Description and analysis of cybercrime in the modern period globally

It is important to note that in the modern legal system, the 1950s and 1990s, the concept of cyber-attack and cybercrime did not exist as we know it today. These are relatively new phenomena that have developed with technological advances and the digitisation of society.

In general, however, information security was not a major issue at that time, as the use of computers and the internet was still relatively limited. However, there were some security incidents and cybercrime, and these played an important role in developing information security and raising awareness of the issue.

The analysis of computer crime in the modern criminal law system reveals a study of computer crime between 1950 and 1990. The 1970^{s} and 1990^{s} saw the emergence of computer crime as a new form of criminal activity. At that time, cybercrime focused primarily on hacking and other forms of unauthorised access to computer systems. However, as technology has evolved, so have the types of cybercrime committed.

Many people associate information security with hackers. Therefore, we are analysing information about hackers and their history. Nowadays, a hacker is understood as an attacker who does something illegal, hacking into some systems for material gain for himself. But this was not always so.

Let's go back half a century to the 1970^{s}, when computers began to gradually enter our lives. Hacking started then, with attempts to misuse technology for its intended purpose. Back then, the concept of a "hacker" was a very enthusiastic person trying to do something non-standard with the system. After all, computer access was mainly for university employees and not so much CPU time was allocated to everyone. You were only allowed to work on the computer a few hours a week on a strict schedule. But even under such conditions, people managed to find time for experiments. Hackers at the time were interested not only in solving some kind of computing problem, but they wanted to understand how certain things worked behind the scenes. Hacking culture emerged from very passionate people.

Computer crime in the modern period was not as widespread and sophisticated as it is today, because information technology was not yet widespread and interconnected. However, a few notable cybercrimes occurred during this period:

- in the 1970^{s}, John Draper, known as "Captain Crunch," discovered a way to get free access to the telephone network through a device made from a

Captain Crunch cereal box;[48]

- the 1971 theft of $10 million from the New York branch of the Union Bank of Switzerland: this was one of the first known examples of computer-assisted bank fraud. Hackers used a computer to bypass the bank's security system and transfer funds to various accounts;

- the 1973 espionage case involving the Soviet Union and the US: a Soviet spy named Vladimir Vetrov stole classified information from the French intelligence agency and used a computer to transmit it to the Soviet Union. It is believed that the information he provided was essential in helping the Soviet Union develop its own stealth technology;

- virus created by student Richard Skrenta in 1981: this was one of the first computer viruses to infect Apple computers. The virus was created as a hoax, but ended up spreading to many computers. This virus spread using floppy disks, which were popular at the time. And because of its ability to clone itself into other environments, it was called the Elk Cloner[49]. But unlike the viruses of our time, it was relatively harmless and only displayed text in poetic form on the monitor;

- in the 1980^{s}, hackers began to exploit government and corporate computer networks, including the ARPANET (predecessor to the Internet) and telecommunications systems. One of the most notorious hacker groups of this period was the Legion of Doom, which attacked the government and large companies including Bell South and American Express;

- in 1983, an American programmer named Clifford Stoll uncovered an attack by a Soviet spy network on the computer system of the Lawrence Berkeley National Laboratory in California. This incident drew public attention to threats to computer security and caused many organisations to improve their computer security;

- in 1986, a student at the University of California, Berkeley, created the first computer virus, called "Brain". It was originally created to stop software piracy, but ended up spreading worldwide, causing serious security problems;

- in 1988, another computer virus called "Morris worm" infected thousands of computers worldwide, causing significant damage. This incident showed that computer security is a major problem and led to the development of stricter protocols for network security.

The Prestel cyber attack of 1983: this was one of the earliest known examples of computer hacking in the UK. A group of hackers gained unauthorised access to the Prestel online service and managed to view and alter sensitive information, including the Royal Family's phone book.

In general, cybercrime during this period was less sophisticated and less

[48] *A brief history of cyber security and hacking*, https://cybernews.com/security/brief-history-of-cybersecurity-and-hacking/, consulted on 1.10.2023.

[49] *Who invented viruses. What is a computer virus*, https://2too.ru/ro/programs/kto-izobrel-virusy-chto-takoe-kompyuternyi-virus.html, consulted on 1.10.2023.

widespread than today, but it contributed to the further development of cyber security and the strengthening of laws that protect personal information and businesses against cyber attacks.

2. Description and analysis of cybercrime in the contemporary legal system

The contemporary criminal law system is facing significant challenges with regard to cybercrime or cybercrime, given the rapid evolution of technology and internet use. Cybercrime involves illegal activities that take place in the virtual environment, such as online fraud, unauthorised access to computer systems, cyber sabotage or distribution of illegal content.

In the contemporary period, there has been a significant increase in cyber-stalking, identity theft and data breaches, with criminals using advanced techniques to gain access to sensitive information and cause harm to individuals and organisations.

In the contemporary legal system, cybercrime presents a number of peculiarities and challenges, namely:

1. technical complexity: cybercrime often involves the use of advanced and sophisticated technologies such as hacking or malware. This brings challenges in identifying and tracking criminals, collecting digital evidence and understanding the technical details involved in the crimes;

2. transnationality: the Internet knows no borders, which means that cybercrime can be committed remotely and offenders can be located in other jurisdictions. This raises issues of jurisdiction and international cooperation in the investigation and prosecution of crime;

3. anonymity and pseudonymity: the use of the internet allows criminals to act anonymously or to hide their real identity behind pseudonyms or false IP addresses. This makes it more difficult to identify and bring criminals to justice;

4. intangible nature of the damage: in the case of cybercrime, damage can be difficult to assess as it is often intangible in nature, such as theft of information, damage to reputation or loss of data. This can affect the prosecution process and damage compensation;

5. speed of technological change: technology is advancing at a rapid pace and cyber criminals are constantly finding new ways to commit crimes. The criminal law system must constantly adapt to these changes and update its legislation to respond to new threats.

Information systems play an essential role in today's society. In general, a computer system is described in terms of a 5-component model: hardware, software, data, usage processes and users.

In the contemporary criminal law system, cybercrime encompasses a spectrum of activities. At one end are offences involving fundamental breaches of personal or corporate privacy, such as: attacks on the integrity of information

held in digital repositories and the use of illegally obtained digital information to blackmail a company or person. Also at this end of the spectrum is the growing crime of identity theft. In the middle of the spectrum are transaction-based crimes such as fraud, trafficking in child pornography, digital piracy, money laundering and counterfeiting. These are specific crimes with specific victims, but the criminal hides in the relative anonymity offered by the internet. Another part of this type of crime involves individuals within corporations or government bureaucracies deliberately altering data either for profit or for political purposes. At the other end of the spectrum are those crimes that involve attempts to disrupt the actual functioning of the internet. These range from spamming, hacking and denial of service attacks against specific websites to acts of cyber-terrorism, i.e. using the Internet to cause public disorder and even death. Cyberterrorism focuses on the use of the internet by non-state actors to damage a nation's economic and technological infrastructure.[50]

Examples of cybercrime include unauthorised access to computer systems, data or identity theft, online fraud, online harassment and other forms of crime involving the use of technology, phishing (obtaining personal information through fraudulent methods), ransomware attacks (locking or encrypting data with a ransom demand), identity theft (fraudulently obtaining and using another person's personal information) or DDoS (denial-of-service) attacks. These crimes are often difficult to detect and track because criminals can operate from anywhere in the world and use sophisticated methods to hide their tracks.

The contemporary criminal law system is based on the idea that crimes should be punished with penalties proportionate to their seriousness and that justice should be applied objectively and impartially.

In recent years, criminal law systems around the world have begun to adapt to the new threats posed by cybercrime. New laws and rules have been developed to deal with cybercrime and law enforcement agencies have begun to improve their capabilities to investigate and prosecute cybercrime.

2.1. Examples of computer crimes in the contemporary criminal law system, 1990s to present

Theft of personal data and invasion of privacy. How does this process take place? For example, in the United States, individuals do not have an official ID card, but a Social Security number that serves as a de facto identification number. Taxes are collected based on this Social Security number from each individual, and many private institutions use the number to keep track of employees, students and patients. Access to a person's social security number provides the opportunity to collect all documents related to that person's citizenship, i.e. to steal their identity. Even stolen credit card information can be used to reconstruct

[50] *Cybercrime*, https://guyanapoliceforce.gy/?page_id=2071, consulted on 1.10.2023.

a person's identity. For example, they could use the credit card information to run up huge bills, forcing credit card companies to suffer huge losses, or they could sell the information to others who can use it in a similar way. Second, they could use individual credit card names and numbers to create new identities for other criminals. For example, a criminal could contact the issuing bank of a stolen credit card and change the mailing address on the account. The criminal can obtain a passport or driving licence with his own photo, but with the victim's name. With a driver's license, the criminal can easily get a new social security card; it is then possible to open bank accounts and receive loans - all with the victim's credit record and history. The original cardholder may not know this until the debt is so large that the bank contacts the account holder. Only then does the identity theft become visible. Although identity theft occurs in many countries, researchers and law enforcement officials are hampered by the lack of information and statistics about the crime worldwide. However, cybercrime is clearly an international problem.

In 2015, the US Bureau of Justice Statistics (BJS) released a report on identity theft. At the time, approximately 1.1 million Americans fraudulently used their identity to open bank accounts, credit cards or utility cards. The report also showed that another 16.4 million Americans were victims of account theft, such as using stolen credit cards and ATM cards. The BJS report showed that while the total number of identity theft victims in the United States has increased by about 1 million since 2012, the total losses suffered by individuals have decreased since 2012 by about $10 billion to $15.4 billion. Most of this decrease was due to a sharp drop in the number of people who lost more than $2,000. Most identity thefts involved small amounts, with losses of less than $300 accounting for 54% of the total.[51]

Computer fraud. Consumer fraud schemes abound on the internet. Among the most famous is the Nigerian scam or "419"; the number is a reference to the section of Nigerian law that the scam violates. Although this confrontation has been used with both fax and traditional mail, the internet has given it a new life. In the scheme, a person receives an email stating that the sender needs help transferring a large sum of money from Nigeria or another distant country. Usually, this money is in the form of an asset to be sold, such as oil, or a large amount of cash that requires "laundering" to hide its source; the variations are endless, and new specifics are emerging. The message asks the recipient to cover some of the costs of moving the funds out of the country in exchange for receiving a much larger sum of money in the near future. If the recipient responds with a cheque or money order, they are told that complications have arisen; more money is needed. Over time, victims can lose thousands of dollars that are completely irrecoverable.

In 2002, IC3 in the U.S. reported that more than $54 million was lost

[51] *Identity theft and financial fraud*, https://bjs.ojp.gov/topics/crime/identity-theft, consulted on 1.10.2023.

through a variety of fraud schemes; this represented a three-fold increase from estimated losses of $17 million in 2001. Annual losses increased in subsequent years, reaching $125 million in 2003, about $200 million in 2006, nearly $250 million in 2008, and more than $1 billion in 2015. In the United States, the largest source of fraud is what IC3 calls "non-delivery/non-delivery", where goods and services are either delivered but not paid for or paid for but not delivered. Unlike identity theft, where theft occurs without the victim's knowledge, these more traditional forms of fraud occur in plain sight. The victim willingly provides private information that enables the crime to be committed; therefore, these are transactional crimes. Few people would believe someone who approached them on the street and promised them easy riches; however, receiving an unsolicited email or visiting an alienating website is different enough that many people easily open their wallets. Despite a great deal of consumer education, Internet fraud remains a growth industry for criminals and prosecutors. Europe and the United States are far from the only sites of cybercrime. South Korea is among the most connected countries in the world, and its cybercrime fraud statistics are growing at an alarming rate. Japan has also seen a rapid rise in similar crimes.

ATM fraud. How does ATM fraud take place? To access an account, a user provides a card and a personal identification number (PIN). Criminals have developed means to intercept both the data on the card's magnetic stripe and the user's PIN. In turn, the information is used to create fake cards which are then used to withdraw funds from the unsuspecting person's account. For example, in 2002, the New York Times reported that more than 21,000 U.S. bank accounts were hacked by a single group engaged in the illegal acquisition of ATM information. One particularly effective form of fraud involved the use of ATMs in shopping malls and convenience stores. These machines are self-contained and not physically part of a bank. Criminals can easily set up a machine that looks like a legitimate machine; however, instead of dispensing money, the machine gathers information about users and only tells them that the machine is inoperable after they have entered PIN codes. Since ATMs are the preferred method for dispensing currency worldwide, ATM fraud has become an international problem.

Electronic fraud. One of the largest and most organized wire fraud schemes was orchestrated by Vladimir Levin, a Russian programmer at a St. Petersburg software company. In 1994, with the help of dozens of confederates, Levin began transferring about $10 million from Citibank, N.A., subsidiaries in Argentina and Indonesia to bank accounts in San Francisco, Tel Aviv, Amsterdam, Germany and Finland. According to Citibank, all but $400,000 was eventually recovered as Levin's accomplices tried to withdraw the funds. Levin himself was arrested in 1995 while in transit at London's Heathrow Airport (at the time, Russia did not have an extradition treaty for cybercrime). In 1998, Levin was finally extradited to the United States, where he was sentenced to three years in prison and ordered to repay Citibank $240,015. Exactly how Levin obtained the

account name and passwords needed was never revealed, but no Citibank employee was ever charged in connection with the case. Because a sense of security and privacy are critical to financial institutions, the exact extent of the wire fraud is difficult to determine.

Spam, steganography and email hacking. Email has spawned one of the most significant forms of cybercrime - spam, or unsolicited advertisements for products and services, which experts estimate accounts for around 50% of emails circulating on the internet. Spam is a crime against all Internet users because it wastes both the storage and network capacity of Internet service providers and is often simply offensive. However, despite various attempts to legislate it away, it remains unclear how spam can be eliminated without violating freedom of speech in a liberal democratic polity. Unlike junk mail, which has an associated postage cost, spam is almost free to the perpetrators - it usually costs the same to send 10 messages as it does to send 10 million.

One of the most significant problems in shutting down spammers involves their use of other people's personal computers. Typically, many machines connected to the Internet are first infected with a virus or Trojan horse that gives the spammer secret control. Such machines are known as zombie computers, and their networks, often involving thousands of infected computers, can be activated to flood the Internet with spam or initiate DoS attacks. While the former can be almost benign, including solicitations to purchase legitimate goods, DoS attacks have been deployed in efforts to blackmail websites by threatening to shut them down. Cyber experts estimate that the United States accounts for about a quarter of the world's 4-8 million zombie computers and is the origin of nearly a third of spam.

Email also serves as a tool for both traditional criminals and terrorists. While libertarians praise the use of cryptography to ensure privacy in communications, criminals and terrorists may also use cryptographic means to hide their plans. Law enforcement officials report that some terrorist groups embed instructions and information in images through a process known as shorthand, a sophisticated method of hiding information in plain sight. Even recognizing that something is hidden in this way often requires considerable amounts of computing power; actually, decoding the information is almost impossible if you don't have the key to separate the hidden data.

In a type of scam called business email compromise (BEC), an email sent to a business appears to be from an executive of another company the business is working with. In the email, the "executive" asks for money to be wired to a specific account. The FBI has estimated that BEC scams have cost US businesses about $750 million.

Hacking. Sometimes email that an organization would like to keep secret is obtained and released. In 2014, hackers calling themselves "Guardians of Peace" released emails from Sony Pictures Entertainment film company executives, as well as other confidential company information. The hackers demanded

that Sony Pictures not release The Interview, a comedy about a CIA plot to assassinate North Korean leader Kim Jong-Un, and threatened to attack theaters that showed the film. After US cinema chains cancelled screenings, Sony released the film online and in a limited theatrical release.

The email hacking even affected the policy. In 2016, Democratic National Committee (DNC) emails were obtained by hackers believed to be based in Russia.

In 2007, Estonian government websites, as well as those for banks and the media, were attacked. The Russian hackers were suspected because Estonia was then in a dispute with Russia over the removal of a Soviet war memorial in Tallinn.[52]

Sometimes a user's or organisation's computer system is attacked and encrypted until a ransom is paid. The software used in such attacks has been called ransomware. The ransom demanded is usually payment in a form of virtual currency, such as Bitcoin. When data is of vital importance to an organisation, sometimes ransom is paid. In 2016, several U.S. hospitals were hit by ransomware attacks, and one hospital paid more than $17,000 to have its systems launched.

Website defacement is a minor issue, however, compared to the spectre of cyber terrorists using the Internet to attack a nation's infrastructure by rerouting air traffic, contaminating water supplies or disabling nuclear power plant safeguards. One consequence of the 9/11 attacks on New York City was the destruction of a major telephone and internet switching centre. Lower Manhattan was effectively cut off from the rest of the world except for radios and cell phones. Since that day, there has been no further attempt to destroy the infrastructure that produces what has been called that "consensual hallucination," cyberspace. Large-scale cyberwarfare (or "information warfare") has not yet occurred, whether initiated by rogue states or terrorist organizations, although both writers and policymakers have imagined this in all too great detail.

In late March 2007, the Idaho National Laboratory released a video demonstrating what catastrophic damage could result from hackers compromising utility systems. Several utilities responded by giving the US government permission to conduct an audit of their systems. In March 2009, the results began to leak out with a report in The Wall Street Journal. In particular, the report indicated that hackers had installed software on some computers that would have allowed them to disrupt electric service. Homeland Security spokeswoman Amy Kudwa said no outages occurred, although additional audits of electric, water, sewer and other utilities will continue.

DDoS attacks. DDoS attacks involve obstructing traffic on websites or other computer systems by overloading them. According to a report by Kaspersky Lab, there were more than 10 billion such attacks in 2020**.**

[52] *Spam, steganography and email hacking*, https://www.britannica.com/topic/cybercrime/Spam-steganography-and-e-mail-hacking, consulted on 1.10.2023.

According to a 2020 report by Juniper Research, the global cost of bank card fraud is estimated to exceed $27 billion by 2025. And according to a 2021 report by Cybersecurity Ventures, the global cost of ransomware attacks is estimated to reach $20 billion by 2025.

Sham-fraud involves the manipulation of large numbers of small amounts of money. In the program that calculates and subsidises interest, certain changes are made to "round down" the subsidised amounts of customers and transfer the amount thus obtained to the criminal's account.

Fraud-Zap is the name of a command (program) that deletes data from a computer's hard drive, of course as a malicious activity.

Uncleanliness. If the computer's internal memory is not cleared after running each program, residual data remains in various locations. Technically, it is possible that a user with access to the computer can read this residual data, which may be confidential, but very rarely can comprehensible data be obtained from it.

Password-scrapers are those programs that record unauthorised passwords used by users.

Piggy substitution. Occurs when an unauthorised person pretends to be an authorised user in order to gain access to a computer or computer network.

Piggybacking are those instructions that allow fraudulent use of computers by removing security barriers.

2.2. Computer crime and COVID-19

Before the COVID-19 pandemic, cybercrime was a major problem for companies and governments around the world. However, the pandemic has led to a significant increase in cybercrime, as many economic and social activities have moved online. In addition, many people faced financial difficulties during the pandemic, which led them to look for ways to make a quick buck through cybercrime.

During the pandemic, cybercriminals took advantage of the opportunities created by working remotely and the weak security of home networks. They carried out attacks using phishing and other social engineering tactics, in which they tried to convince victims to reveal personal information or click on malicious links.

Cybercriminals also used new methods to take advantage of the pandemic. For example, there have been reports of cyber-attacks on hospitals and companies that manufacture protective equipment, as well as an increase in fake websites claiming to provide information about COVID-19 but actually trying to install malware or obtain personal information.

The COVID-19 pandemic has changed the way people work, communicate and interact, which has had a significant impact on cybercrime.

Before the COVID-19 pandemic, cybercrime was already a major concern for authorities around the world, but the pandemic has amplified this problem. With the implementation of social distancing measures and remote working, more companies and organisations have become vulnerable to cyber attacks and other forms of cyber crime. Employees working from home may use insecure networks, making data and information more vulnerable.

As the pandemic has continued, criminals have found new ways to take advantage of people. A number of cyber attacks have been reported that have been linked to the pandemic, such as phishing campaigns involving the provision of false information about the virus or the sale of fake products, such as protective medical equipment.

In addition, the pandemic has accelerated the shift to digitalisation in many sectors, such as financial services, which has created new opportunities for cybercriminals. More cases of online financial fraud have been reported, as well as theft of personal data and bank accounts.

In response to this increased threat, governments and organizations have begun taking steps to protect data and information, such as implementing stronger cybersecurity programs, training employees to identify and report cyberattacks, and developing new laws and rules to protect personal data and punish cybercriminals.

In terms of efforts to prevent and combat cybercrime, the pandemic has led to increased efforts by governments and companies to protect networks and reduce the risks of cyberattacks. In addition, the pandemic has highlighted the importance of cybersecurity and prompted.

By 2020, cybercriminals were attacking the networks and computer systems of individuals, companies, and even global organizations in droves. The number of cybercrime victims increased dramatically by 69% in 2020 during the COVID-19 pandemic compared to 2019, from nearly 467,000 victims per year to 792,000.

The number of people under 20 falling victim to cybercrime has increased 100% during the pandemic, thanks to online surveys, from an average of 10,000 per year in 2019. Could have been reduced due to shifting focus on health crisis.

2.3. Analysis of statistical data on cybercrime

Let's look at the data in the **Fig. 3.** *Most types of cybercrime reported worldwide in 2022, by number of people affected*. According to it, in 2022, the most common type of cybercrime reported to the US Internet Crime Complaint Center was phishing, which affected approximately 300,497 people. In addition, nearly 59 thousand personal data breach cases were reported to IC3 in that Precedent. Card fraud was also reported to the tune of 22 985 cases.

Fig. 3. *Most types of cybercrime reported worldwide in 2022, by number of people affected*

2022 CRIME TYPES

By Victim Count

Crime Type	Victims	Crime Type	Victims
Phishing	300,497	Government Impersonation	11,554
Personal Data Breach	58,859	Advanced Fee	11,264
Non-Payment/Non-Delivery	51,679	Other	9,966
Extortion	39,416	Overpayment	6,183
Tech Support	32,538	Lottery/Sweepstakes/Inheritance	5,650
Investment	30,529	Data Breach	2,795
Identity Theft	27,922	Crimes Against Children	2,587
Credit Card/Check Fraud	22,985	Ransomware	2,385
BEC	21,832	Threats of Violence	2,224
Spoofing	20,649	IPR/Copyright/Counterfeit	2,183
Confidence/Romance	19,021	SIM Swap	2,026
Employment	14,946	Malware	762
Harassment/Stalking	11,779	Botnet	568
Real Estate	11,727		

Descriptors*			
Cryptocurrency	31,310	Cryptocurrency Wallet	20,781

*These descriptors relate to the medium or tool used to facilitate the crime and are used by the IC3 for tracking purposes only. They are available as descriptors only after another crime type has been selected. Please see Appendix B for more information regarding IC3 data.

Source: https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf

The Federal Bureau of Investigation (FBI) issued a report on internet crime in 2022, showing that ransomware cyber attacks violated the networks of at least 860 organisations with critical infrastructure, with losses of about $34.3 million. The number of victims represents only attacks reported to the Internet Crime Complaints Centre (IC3), with the actual number considered to be higher.[53]

Next, we analyse from the **Fig. 4.** *IC3: total damage caused by cyber-crime reported 2018-2022* and conclude the following: between 2021 and 2022, the amount of monetary damage caused by cybercrime reported to the Internet Crime Complaint Centre (IC3) increased significantly. In the last reporting period, annual losses from complaints to IC3 amounted to $10.3 billion in 2022, up from $6.9 billion in 2021.[54]

Percentage of internet users in selected countries who have ever experienced any cybercrime in 2022 is shown in **Fig. 5**. According to this, in 2022, about four out of ten internet users worldwide have ever experienced cybercrime. Based on a survey conducted between November-December 2022, internet users in India were most likely to have fallen victim to cybercrime, as nearly 68% of respondents claimed to have ever experienced cybercrime. The United States

[53] https://www.bleepingcomputer.com/news/security/fbi-ransomware-hit-860-critical-infrastructure-orgs-in-2022/, consulted on 1.10.2023.

[54] https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf, consulted on 1.10.2023.

ranked second, with nearly half of respondents, 49 %, saying they had experienced cybercrime. Internet users in Japan have the lowest percentage, at 21 percent. That would roughly mean that 1 in 4 Internet users in Japan has been affected by a cybercrime. That's a pretty worrying statistic.

Fig. 4. IC3: total damage caused by computer crimes reported 2018-2022

Source: https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf

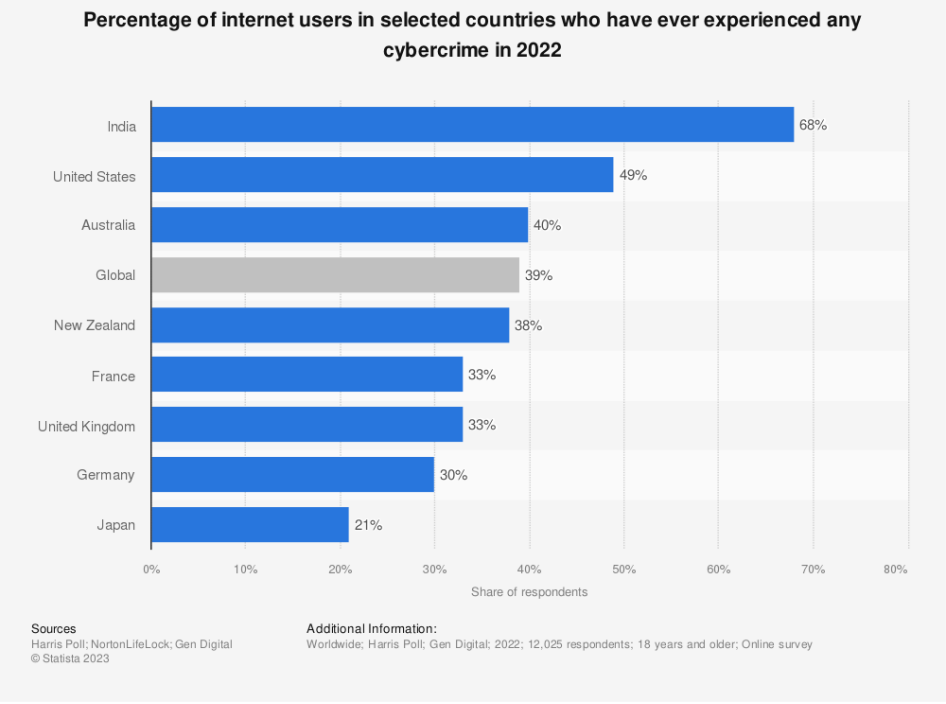
In **Fig. 6.** *Evolution of Malware Attacks from 1984 to 2018*, a survey conducted by the AV-TEST company, we see a sharp increase in cybercrime, malware attacks from 2013 to 2018, when the number of such attacks practically doubled. If in 2012, malware attacks globally were around 100 million annually, then in 2016 these attacks amounted to about 600 million, and in the year more than 700 million attacks reported annually.[55]

In **Fig. 7** we analyze *Distribution of cyber attacks across worldwide industries in 2022* and find that globally, manufacturing had the highest share of cyber attacks among the leading industries worldwide. During the year under review, cyber attacks in manufacturing companies accounted for nearly 24.8% of all cyber attacks. Finance and insurance followed with about 18.9 percent. Professional, business and consumer services ranked third with a share of 14.6 percent. Transportation services garnered a 3.9 percent share and education services

[55] https://www.av-test.org/en/, consulted on 1.10.2023.

7.3 percent. This is a worrying statistic, especially for companies active in manufacturing and consulting services.[56]

Fig. 5. Percentage of internet users in selected countries who have ever experienced any cybercrime in 2022



Source: https://www.statista.com/statistics/194133/cybercrime-rate-in-selected-countries/

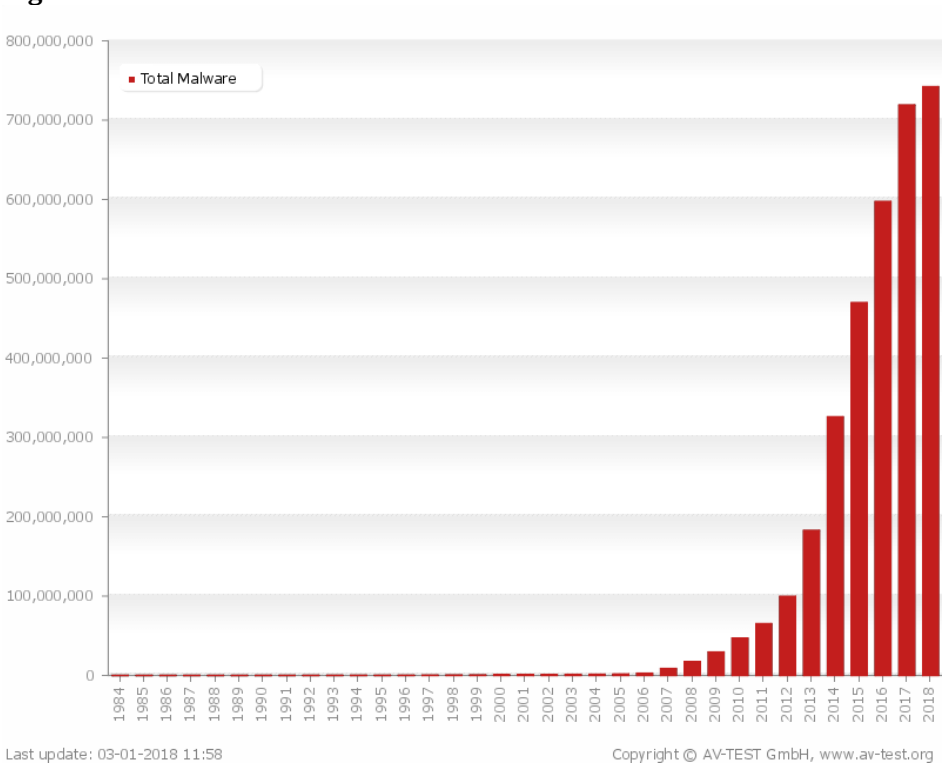
Committing a cybercrime can have serious consequences. In the U.S., for example, a cybercriminal can get up to 20 years in prison for breaking into a government institution if it compromises national security. Yet despite the consequences, cybercriminals continue to wreak havoc across the globe. But some countries seem to be targeted more than others.

In **Fig. 8** we look at the countries that have suffered the most significant cyber attacks between 2006 and 2020, an analysis by Specops Software. Specops Software is the leading provider of password management and authentication solutions for enterprises. They are responsible for secure user authentication. Using data from Specops Software, we can conclude that the top place is the US, with 156 serious cyber attacks recorded. That's an average of 11 significant attacks per

[56] https://xontech.md/news/statisticile-atacurilor-cibernetice-pentru-anul-2021-la-nivel-mondial/, consulted on 1.10.2023.

year, which is more than Russia has had in 14 years.[57]

Fig. 6. Evolution of malware attacks between 1984 and 2018



Source: https://www.av-test.org/en/

While there are many different types of cyberattacks, Specops highlights the four most commonly used for significant cybercrime:

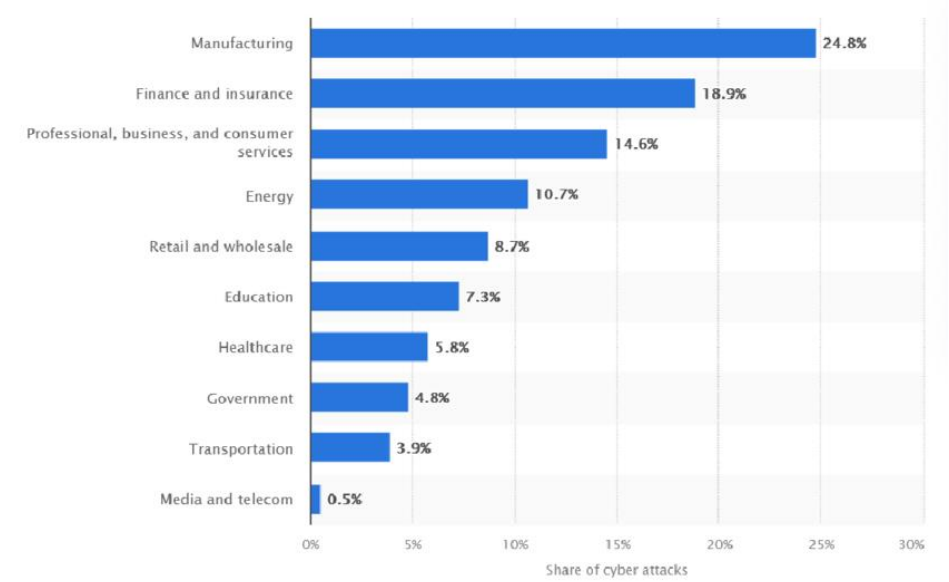
- *Structured Query Language (SQL) injection attack.* SQL is code used to communicate with a database. In a SQL injection attack, the hacker writes vindictive SQL code and inserts it into the victim's database to access private information.

- *Man in the middle (MITM).* This form of attack occurs when a cybercriminal accesses a communication channel between two people and eavesdrops on their online exchanges.

- *Phishing attacks.* When a cybercriminal poses as a legitimate institution and emails a victim to obtain personal details such as login details, home address, credit card information.

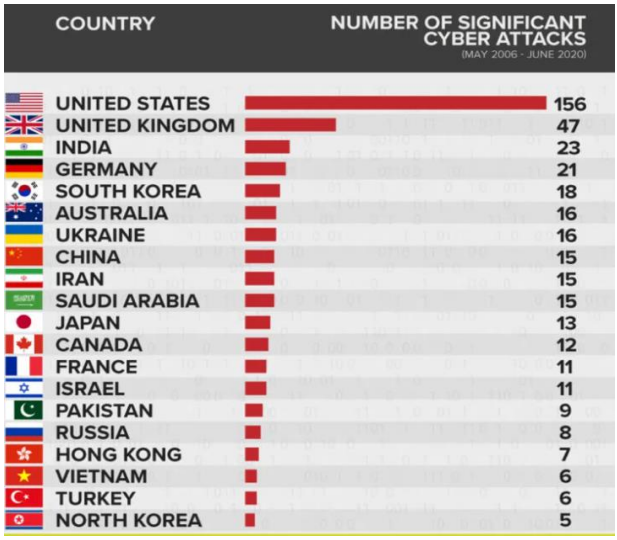
[57] https://specopssoft.com/blog/countries-experiencing-significant-cyberattacks/#:~:text= Specops%20Software%20found%20that%20the,alone%20occurring%20throughout%20the%20year, consulted on 1.10.2023.

Fig. 7. Distribution of cyber attacks across worldwide industries in 2022



Source: www.statista.com/statistics/1315805/cyber-attacks-top-industrie s-worldwide/

Fig. 8. Countries that suffered the most significant cyberattacks between 2006 and 2020



Source: https://specopssoft.com/blog/countries-experiencing-significant-cyber-attacks/#:~:text=Specops%20Software%20found%20that%20the,alone%20occurring%20throughout%20the%20year.

- *Denial of service (DoS) attack.* This involves flooding a victim's system

with traffic to the point where their network is inaccessible. The hacker does not gain valuable information from this style of attack.

With the ubiquity of smartphones and social networks reporting our every move, it's not surprising that cybercrime is on the rise.

We conclude that, **currently, the most common cybercrimes worldwide are the following**:

- Phishing: phishing is when criminals send fraudulent emails pretending to be from legitimate companies in an attempt to collect sensitive personal information. Often, any link in the email will redirect to a website owned by the scammer, so always be careful what information you provide online.

- Harassment: cyber actors use electronic communication such as email, social media or websites to stalk and harass people. Forms of online harassment include slander, libel, false accusations, threats or any other behaviour that demeans or embarrasses someone. Penalties for cyberstalking can include substantial fines and even imprisonment.

- Ransomware: cybercriminals can install malicious software on your system that will essentially hold your important information hostage until you meet their demands. A typical ransomware attack will shut down a victim's computer or encrypt their files, agreeing to release them only if the victim pays a ransom. However, all too often, files are never recovered.

- Child pornography: the National Center for Missing and Exploited Children has received more than 10 million reports of suspected child sexual exploitation in the last year alone. Perpetrators will use the internet to access sexually explicit images of children and sometimes even arrange for a face-to-face meeting.

- Theft of intellectual property: more commonly known as piracy, the internet abounds with books, music, movies and more that have been illegally obtained and made available for free download. Despite what some people say, piracy is not a victimless crime. Not only do artists and creators lose out, but many illegal downloads also contain hidden malware that can destroy your computer and steal your personal data.

- Account hacking. We all know how important it is to guard our passwords - think of the damage someone could do if they gained access to your email account containing all your most personal information. If someone logs on to your email, social networks or computer without authorisation, they could face jail time.

- Credit card fraud. Half of all credit card fraud starts with spyware, malicious software unknowingly installed on the victim's computer or mobile device. Spyware runs in the background, collecting your data and sending it back to the criminal, who then uses your card to make fraudulent purchases.

In conclusion, we see that the number of cybercrimes is constantly increasing. But at the same time, there is a strong focus on the importance of cyber security, at the organisational level, at the country level, and trying to stop it.

2.4. Latest cybercrime and cyberattacks worldwide in year 2023

Texas banking institution compromised in cyber attack. The SNNs of over 17,000 US residents have been exposed after a financial company employee's email account was compromised in a cyber attack. According to bank officials, the loss of SSNs poses significant risks, as impersonators can use the stolen data in tandem with names and driver's license numbers for identity theft[58].

A private university in Bluefield, Virginia, suffered a cyber attack that affected IT systems and caused all exams to be postponed. Following a ransomware attack, the institution's emergency broadcast system was hijacked, and students and employees were informed via text messages and email alerts that their data had been stolen and would be released if the institution paid a ransom. Additional alerts shared links and instructions about visiting the ransomware group's data leak site to see additional messages about the attack and any leaked data[59].

An American security researcher has discovered an access vulnerability in Toyota's management system. Toyota's Global Supplier Preparation Information Management System (GSPIMS) was breached by a security researcher who responsibly reported the company's problem. GSPIMS is the automaker's web-based application that allows employees and suppliers to remotely connect and manage the company's global supply chain. The security researcher discovered a "back door" in Toyota's system that allowed anyone to access an existing user account as long as they knew their email. Through an intrusion test, the researcher discovered he could freely access thousands of confidential documents, internal projects, supplier information and more. A system administrator on GSPIMS can access sensitive information such as classified documents, project schedules, supplier rankings and data of over 14,000 users.[60]

Chinese cyber espionage group Moshen Dragon attacks Asian companies. Cybersecurity researchers have identified a new group of malicious cyber activity tracked as Moshen Dragon targeting telecommunications service providers in Central Asia. While this new threat group has some overlap with "RedFoxtrot" and "Nomad Panda", including the use of ShadowPad and PlugX malware variants, there are enough differences in their activity to track them separately. According to a new Sentinel Labs report, Moshen Dragon is a skilled hacking group with the ability to adjust its approach depending on the defenses it faces[61].

---

[58] *Texas bank error that exposed thousands of Social Security numbers*, https://cybernews.com/news/happy-state-bank-breach/, consulted on 1.10.2023.

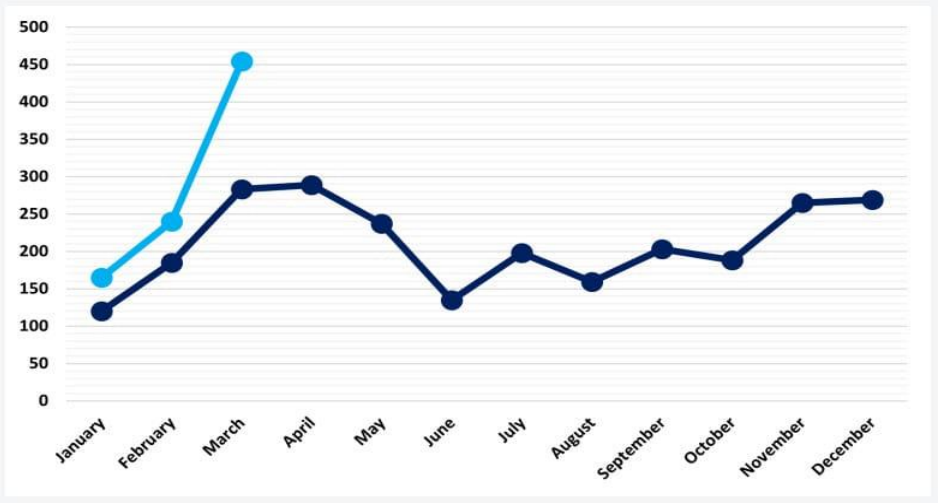
[59] *Private university in the USA suffered a cyber attack*, https://www.bleepingcomputer.com/news/security/ransomware-gang-hijacks-university-alert-system-to-issue-threats/, consulted on 1.10.2023.

[60] *An American security researcher has discovered an access vulnerability in Toyota's management system*, https://www.bleepingcomputer.com/news/security/researcher-breaches-toyota-supplier-portal-with-info-on-14-000-partners/, consulted on 1.10.2023.

[61] Cyber security news, https://stisc.gov.md/ro/noutatile-saptamanii-din-cybersecurity-6052022,

A new record of ransomware attacks in March 2023. According to a report released by the NCC Group, 459 ransomware cyber attacks were reported worldwide in March this year, according to **Fig. 9**. The report, based on its own statistics, shows that the figure is a new record, 91% more than the previous month and 62% more than March 2022, and also the highest number of hacking incidents and data leaks recorded in the last three years.[62]

Fig. 9. A new record of ransomware attacks in March 2023, according to a report released by NCC Group



Source: www.bleepingcomputer.com/news/security/march-2023-broke-ransomware-attack-records-with-459-incidents/

There are many **computer fraud** schemes currently being witnessed worldwide:

1. Investment fraud, where criminals try to get money from their victims. Here are some of the most common fraud schemes in the contemporary legal system:

- *Ponzi schemes.* These schemes involve promises of investments with very high returns, but which are not sustainable in the long term. Investors are paid out of other investors' money and not from the profits of the real investments. This type of scheme often requires investors to bring in other investors, and cybercriminals may use websites or emails to promote these schemes.

consulted on 1.10.2023.

[62] March 2023 broke ransomware attack records with 459 incidents, https://www.bleepingcomputer.com/news/security/march-2023-broke-ransomware-attack-records-with-459-incidents/, consulted on 1.10.2023.

- ***Fake stock trades.*** Cybercriminals may create fake websites or documents that appear to be from a reputable company in order to attract investors. These can be used to promote counterfeit stock trades or to encourage investors to buy shares that do not exist or are invalid.

- ***Cryptocurrency investment schemes.*** Cybercriminals can use cryptocurrencies to initiate fraudulent investment schemes. These may involve promises of high returns or opportunities to buy cryptocurrencies at very low prices. In reality, these schemes are often deceptive and cybercriminals use their victims to get money.

- ***Investment phishing schemes.*** Cybercriminals may use spoofed emails or websites to promote investment schemes that appear to be from reputable companies. These messages may contain links to fake websites that ask investors to enter personal and confidential information, such as credit card numbers or passwords.

- ***Cryptojacking.*** This involves using other people's computers without permission to mine cryptocurrencies. Cybercriminals can infect other people's computers with malware or use infected websites to take control of computers.

It's important to be wary of such fraud schemes and do your research before making an investment. Always check websites before making an investment and do not provide personal or confidential information unless you are sure the message is legitimate. It is also important to have anti-virus software installed and update it regularly to prevent such cybercrime.

2. Business/employment type computer fraud:

- ***CEO Fraud.*** This crime involves a cyber attack in which criminals pose as an executive director or CEO of the company and request a financial transaction or money transfer to an account controlled by the criminals. This method of fraud is often used in large money transactions and requires careful preparation of the message and fake websites to be credible.

Phishing. This fraud method involves sending forged emails to company employees in order to convince them to disclose confidential information or conduct financial transactions. These emails are often highly credible and may contain links to fake websites that appear genuine but are used to retrieve information.

Ransomware. This method of cybercrime involves infecting computers with malware that blocks access to files or entire systems. Criminals then demand a ransom to unlock the files or systems. This method of fraud can severely damage a company's business and have a significant financial impact.

False Invoice Fraud. This method of fraud involves sending false invoices to companies for services or products that were never delivered. Criminals may use fake email addresses or phone numbers to mislead company employees into paying the invoices.

Cyber security breach. This method of cybercrime involves penetrating a company's security systems to access confidential information or to introduce

malware. Criminals can then use this information to conduct fraudulent financial transactions or disrupt the company's business.

To prevent these types of crimes, it's important to have a strong cyber security system and provide security training to employees. Employees need to be trained to recognize cyber attacks and understand the importance of keeping information confidential. It is important to monitor systems and install security updates in a timely manner to protect against vulnerabilities.

According to the „Data Breach Investigations Report"[63] 32% of data breaches in 2022 were associated with phishing. Thus, international experts are of the opinion that phishing will become more prevalent in the coming years and its scale will increase considerably. Another example that demonstrates this is the fact that in 2021, more than 60,000 phishing websites were created every month, and the loss of data and the consequences of this shows the following alarming statistics:

- one of eight employees share information on a phishing site;
- 97% of users cannot recognise a sophisticated phishing email;
- 95% of all attacks targeting a company's infrastructure are caused by phishing;
- only 3% of employees report phishing emails to management.
- a single phishing attack globally results in an average loss of $1.6 million.
- 30% of phishing emails are opened by users and 12% of these users click on the infected link or attachment;
- 85% of all organisations have been affected by a phishing attack at least once;
- mobile phishing attacks are different from traditional phishing attacks and much more problematic;
- 81% of all mobile phishing attacks were launched outside of email;
- the number of phishing emails containing some form of ransomware has increased to 97.25%;
- 96% of all targeted phishing attacks are aimed at collecting information;
- one in every 2 organisations that fell victim to a ransomware attack in 2019 had 73% of their data successfully encrypted and recovery was impossible;
- one in 3 companies that fell victim to a ransomware attack paid ransom to recover data, and the average ransom paid globally was nearly $84,000.

Taking all of this into consideration, companies need to implement and invest in comprehensive user safety awareness programs in the online space. Furthermore, organisations should implement simulators that can explain to employees how to recognise new phishing methods.

[63] *Cyber Breach Investigations Report*, Verizon 2022, https://www.verizon.com/business/resources/reports/dbir/2022, consulted on 1.10.2023.

2.5. Global cybercrime statistics for 2022[64]

Cybercrime statistics show that at least 422 million people have been affected, according to FBI internet crime records, with 800,944 complaints recorded in 2022. Nearly 33 billion accounts will be breached in 2023, with the cost of these breaches estimated at $8 trillion.

The internet can be a scary place, full of scammers, thieves and saboteurs. That's no exaggeration. According to the Norton Cyber Security Insights Report, more than 143 million Americans in 2022 were affected by cybercrime in the past year, with 80% of those surveyed reporting that they or someone they knew had been victimized.[65]

The cost of cybercrime is estimated to reach $10.5 trillion by 2025, up from $6 trillion in 2022. It is said that 80% of reported cybercrime is generally attributed to phishing attacks.

The percentage of attacks against organisations by continent in 2021 is as follows[66]:

- the UK had the highest number of cybercrime victims per million internet users at 4783 in 2022, up 40% on 2020 figures;
- the country with the highest number of victims per million internet users in 2022 was the US at 1494, a 13% decrease from 2020;
- 1 in 2 internet users in North America had their accounts stolen in 2021;
- the UK and US disproportionately had more cybercrime victims per million internet users compared to other countries - the US had 759% more victims in 2021 than the next highest country, Canada;
- the Netherlands saw the biggest increase in victims - 50% more than in 2020;
- Greece saw the biggest decrease in casualties - by 75% in 2020;
- over the period May 2020-2021, cybercrime in the Asia-Pacific region increased by 168%. Japan saw a 40% increase in cyber attacks in May 2021 compared to the previous months of that year;
- 76% of respondents in a 2022 case study covering the US, Canada, UK, Australia and New Zealand say their organisation suffered at least one cyber attack this year. That's up from 55% in 2020;
- from the same survey, only 30% have cyber insurance, and 69% fear that a successful cyber attack could put their SME completely out of business;
- in 2021, Asian organisations suffered the most attacks globally. The percentage of attacks against organisations by continent in 2021 is as follows: Asia (26%), Europe (24%), North America (23%), Middle East and Africa (14%)

---

[64] Latest cybercrime statistics, https://aag-it.com/the-latest-cyber-crime-statistics/, consulted on 1. 10.2023.

[65] Most common cybercrimes, https://www.enkanter.com/article/9-most-common-computer-and-internet-cyber-crimes, consulted on 1.10.2023.

[66] https://aag-it.com/the-latest-cyber-crime-statistics/, consulted on 1.10.2023.

and Latin America (13%);

- in Asia, the main type of attack experienced was server access, with 20% of attacks observed. This was ahead of ransomware (11%) and data theft (10%);

- in Europe, ransomware was the main type of attack, accounting for 26% of attacks on the continent. Server access attacks (12%) and data theft (10%) were the next most common attack types;

- in North America, ransomware was also the main type of attack, with 30% of attacks. This was ahead of business email compromise (12%) and server access attacks (9%);

- in the Middle East and Africa, the main type of attack observed was server access, accounting for 18% of attacks. Server access attacks were also observed in 18% of attacks, followed by misconfigurations (14%);

- in Latin America, the main type of attack was ransomware, accounting for 29% of attacks. This was before business email compromise and credential harvesting (both observed in 21% of attacks);

- the US Department of IC3 has received reports from 24,299 victims of cybercrime. This amounted to over $956 million lost;

- romance scams and confidence fraud are prevalent in the US - IC3 received reports from 24,299 victims in 2021, with losses amounting to over $956 million. 32% of victims were over 60 - the highest proportion of victims in 2021. 16% were aged 50-59. Only 2% were under 20;

- sextortion is another widespread problem in the US. Cybercriminals threaten to publish photos, videos or sensitive information involving sexual acts of victims if their demands are not met. The IC3 department received over 18,000 complaints in 2021 related to sextortion. Victim losses totaled more than $13.6 million.

- potential losses from cybercrime by U.S. individuals in 2022 totaled over $10.2 billion. This is significantly higher than in 2021, when individuals lost about $6.9 billion. Given that there were 5% fewer complaints in the U.S. in 2022 than in 2021, this suggests that cybercrime cost more per victim than the previous year.

3. Prevention of computer crimes

Cybercrime prevention is a topic of great importance in today's digital world. To prevent cybercrime, here are some important steps you can take:

- back up all your important files and store them independently of your system (e.g. in the cloud, on an external drive);

- check the software and all systems used;

- make sure you have the latest antivirus software installed on your computer and mobile devices;

- install security software: Make sure you have up-to-date security software installed and that you update regularly to protect against viruses, spyware and other

cyber threats;

- use strong passwords: Use strong passwords that include a combination of letters, numbers and special characters. Avoid using the same passwords for multiple accounts and change passwords at regular intervals;

- protect your personal data: Don't provide personal or financial information on unsafe sites or to strangers. Make sure your personal and financial information is stored in a safe place and protected with strong passwords;

- pay attention to warning messages or security alerts asking you to update your information or enter login information. These could be phishing attacks. Phishing is a common method of cyber attack, where criminals pose as trusted individuals or organisations and ask for your personal or financial information;

- be aware of suspicious emails or messages and do not provide personal information to people or sites you do not know;

- do not leave your computer or mobile device unattended in public places or open offices;

- learn about the latest cyber threats and how to protect yourself against them by watching security news and attending training courses;

- use only licensed and up-to-date software. Pirated software may contain viruses or other cyber threats;

- avoid using public Wi-Fi networks for banking, online commerce or personal business;

- be careful on public Wi-Fi networks: Avoid using public Wi-Fi networks to access personal or financial information. These networks are insecure and can be used by criminals to access your information;

- be careful with USB devices: Don't use USB devices from unknown or unsafe people as they may contain viruses or other cyber threats;

- educate yourself about cyber security and be aware of new trends and attack methods. Be prepared to protect yourself against evolving cyber threats;

- disable third-party or outdated components that could be used as entry points;

- download mobile apps or any other software only from trusted platforms;

- talk to your family - including your children - about staying safe online;

- regularly check and update the privacy settings on your social media accounts;

- update your passwords and make sure they are strong (a mix of capital letters, small letters, numbers and special characters);

- don't click on links or open attachments in emails you don't expect to receive or from an unknown sender.

By following these steps, you can significantly reduce the risk of becoming a victim of cybercrime. Also, if you think you are a victim of a crime, alert your local police.

Chapter IV.
Conclusions and recommendations

Comparing cybercrime in the modern and contemporary period can be approached from several perspectives, including reports, statistics and relevant events. It is important to assess the evolution of cybercrime in this context, as well as how legal systems and technology have evolved to prevent and punish it.

The increase in the seriousness of cybercrime is also evident in the types of penalties imposed on offenders. In the modern period, penalties for cybercrime were relatively light, with fines and short prison sentences being the norm. However, in contemporary times, penalties have become much harsher.

The paper analysed and compared modern and contemporary approaches to cybercrime in the criminal law system. It was found that although there are differences in the definitions, preventive measures and sanctions applied in different legal systems, there are also a number of similarities. In order to combat cybercrime effectively, a global approach and collaboration between different countries and organisations is needed.

A comparative analysis of cybercrime in the modern period compared to the contemporary period reveals an increase in the frequency and seriousness of such crimes, as well as changes in the types of crimes committed, with more emphasis on cyberstalking, identity theft, and data breaches. These findings are supported by statistics and reports from law enforcement agencies, cybersecurity firms, and other organizations tracking cybercrime trends.

Cybercrime is currently the fastest growing type of crime worldwide. The financial losses caused by cybercrime exceed the total losses from the global trade in all illicit drugs. Not surprisingly, individuals and organisations operating on the internet are wary of potential hacking scenarios and data leaks. In addition to financial losses, cyber-attacks also affect organisations' reputations.

The information technology revolution has given rise to unprecedented economic and social changes, but at the same time it also serves less legitimate purposes: the emergence of new crimes, or the perpetration of traditional crimes through new technology. Existing legal concepts are being challenged by the emergence of new technology. Often the place where the crime is committed differs from where the offender is located. At the touch of a button, they can trigger catastrophes thousands of miles away. These crimes damage the assets of organisations, institutions and individuals. Legal regulation aims to protect computer systems and the data stored on them from unauthorised access.

In conclusion, a comparative analysis of cybercrime in the modern period compared to the contemporary period reveals a significant increase in the frequency and seriousness of such crimes, with cyberstalking, identity theft and data breaches emerging as major forms of criminal activity. These findings are supported by statistics and reports from law enforcement agencies, cybersecurity

firms and other organisations tracking cybercrime trends. As technology continues to evolve, cybercrime is likely to become even more sophisticated, highlighting the need for continued efforts to prevent and punish such crimes.

It can be concluded that cybercrime is a major challenge for the contemporary criminal law system and that tackling it requires a concerted effort from authorities around the world. However, significant progress is being made in the fight against these crimes and the current criminal law system is trying to adapt to these new threats.

Chapter I has presented theoretical aspects of cybercrime. Cybercrime has been defined and the history and evolution of cybercrime worldwide has been described. Of course, all types of cybercrime were also specified.

In Chapter II, practical aspects of cybercrime in the modern and contemporary criminal law system were presented. It described in detail how the harmonisation of cybercrime legislation is taking place worldwide. For a broader study, cybercrime in the Republic of Moldova was also analysed. A comparative analysis of the sanctions imposed in the modern and contemporary criminal law system was also carried out.

Chapter III describes the known cybercrimes in the modern and contemporary law system. A list of recommendations for the prevention of cybercrime has also been drawn up.

As cyberspace is the fifth common space, after land, sea, air and space, cybercrime requires coordination, cooperation and specific regulatory measures, not only at national but also at international level (including operational cooperation and the creation of regional bodies to combat it), and it is not enough to develop appropriate legislation at national level.

The countries of the world will need to continue their efforts to harmonise legislation worldwide. This would help to reduce legal loopholes, which allow criminals to avoid criminal liability in one country by moving their illegal activities to another country with more lenient legislation. Finally, harmonisation of cybercrime legislation worldwide could improve international law enforcement cooperation and help prevent and combat transnational cybercrime.

In addition to the recommendations for avoiding cybercrime set out above, the following are proposed for consideration:

- we need to educate ourselves and be prepared in the fight against cybercrime. To be one step ahead of the criminals. This has to start with the gadgets we use every day;
- similarly, we need to secure our IT and office technology in the organisations where we work;
- to care about the people around us and to react if we understand that they could become victims of cyber criminals;
- we would welcome TV shows, commercials where we talk about the most common cybercrimes and how not to become victims ourselves;
- as children have access to gadgets from a very young age, they should

be taught about potential risks and online behaviour in kindergarten, school, etc.

- it is recommended that the subject of law be included in the curriculum. Whether in general or in depth, pupils need to know about all crimes, as some learn about them only after they have committed them. Thus, educating and informing the younger generation correctly would only bring advantages.

On the legal front, the following actions are recommended to reduce cybercrime:

- tougher penalties (doubling the penalties would be the recommendation), at least for a few years to minimise cybercrime;
- there is a need for our country to have a state organization/agency, which would regulate and monitor all cybercrimes;
- it would also be welcome to set up a professional Association of cyber/electronic information security specialists, managers and auditors at the local level to increase the qualification of cyber security specialists;
- it would be good if our country would host international events/seminars and other events organised on cyber security. That way we will grow, cyber security specialists will evolve and provide a higher degree of protection and safety from cybercrime;
- there is a need for the Government to establish a Cyber Crisis Management Plan, specifically a crisis management plan for large-scale cyber incidents. The risks are enormous in this day and age and we need to be prepared for anything.

Bibliography

I. Books and articles

1. Begu, V., *Cybercrime*, http://www.academia.edu/9204220/CRIMINALITATEA_INFORMATI C%C4%82, consulted on 1.10.1023.
2. Branza, N., State, V., *Treatise on Criminal Law. Special Part*, volume II. Chisinau: Tipografia centrala, 2015.
3. Brazhnik, S.D., *Crimes in the field of computer information: Educational method. development according to a special course* / Comp. S.D. Hawkmoth. Yaroslavl: Yarosl. state Univ., 2000.
4. Crijanovschi, S. *Some aspects of comparative legal-criminal analysis of computer crimes in the criminal law of the Republic of Moldova and Romania*. In: Studia Universitatis Moldavia. Series "Social Sciences", 2016, no. 3(93).
5. Florescu, V., Florescu G., *Analysis of computer crimes criminalized in the current legislation and in the perspective of the new penal cod*e, in: Romanian Journal of Informatics and Automatics, vol. 22, no. 2, 2012.
6. General Secretariat of the European Council, *Internal Security Strategy of the European Union: Towards a European Security Model*, Luxembourg: Publications Office of the European Union, ISBN 978-92-824-2690-6.
7. Gercke, M., *Understanding cybercrime: phenomena, challenges and legal response*, ITU 2012.
8. Grigoriev A. N., Meshkov V. M., Protsenko N. Yu., *Computer crimes and computer information protection. Scientific and practical manual*, Kaliningr Publishing House. Judicial Institute of the Ministry of Internal Affairs of Russia, Kaliningrad, 2003.
9. Introductory guide to the application of legal provisions on cybercrime / Ministry of Communications and Information Technology, Bucharest, 2004.
10. Introductory guide to the application of legal provisions on cybercrime / Ministry of Communications and Information Technology. Bucharest, 2004.
11. Ioniță, G. I., *Cybercrime offences: criminalisation, investigation, prevention and combating*. Bucharest: Universul Juridic, 2011.
12. Krilov, V.V. *Investigation of crimes in the sphere of information*. Moscow: Gorodets, 1998.
13. Lazari, C. *Some aspects of cyberterrorism*, in: Scientific and Practical Review of the Institute of International Relations of Moldova, no.1, 2016.
14. Milodin D., Sbora C., *Non-security - a prerequisite for cybercrime*. Theoretical and applied economics. Volume XIX (2012), No. 4(569).
15. Milodin, D., Sbora C., *Non-security - premise of cybercrime. Theoretical and applied economics*. Volume XIX (2012), No. 4(569).
16. Moise, Adrian Cristian, *Methodology of forensic investigation of computer crimes*, Universul Juridic Publishing House, Bucharest 2011.
17. Motskobili, I., *Hackers are striving for world domination*. in: Komersant – Daily, 1998, no. 73.
18. Popova, V. I. (ed.)., Object-structural analysis of organized criminal activity in the field of private investment: textbook, Moscow, 1997.

19. Schonberg, S., *Computer-related crime*, Conference "Challenges of Cybercrime", Council of Europe, Strasbourg, 15-17 September 2004, available at http://www.cybercrimelaw.net/documen ts, consulted on 1.10.2023.
20. Sfetcu N., *Beginner's Guide for Cybercrime Investigators*, MultiMedia Publishing, ISBN: 978-606-033-093-6, 2014.
21. Spânu-Dumneanu, L., *International and national developments in the field of cybercrime*, https://juridicemoldova.md/6687/evoluarile-internationale-si-natio nale-in-domeniul-infractiunilor -informatice-lsd.html, consulted on 1.10.2023.
22. Talpă, Boris, *Brief incursion into the characteristics of computer crimes*, https:// juridicemoldova.md/6987/scurta-incursiune-in-caracteristica-criminalistica-a-infractiunilor-informatice.html, consulted on 1.10.2023.
23. Vekhov, V.B., Golubev V.A., *Investigation of computer crimes in the CIS countries*: monograph, ed. B.P. Smagorinsky. Volgograd: VA Ministry of Internal Affairs of Russia, 2004.

II. Normative acts

1. Romanian Law on some measures to ensure transparency in the exercise of public office, public functions and in the business environment, prevention and sanctioning of corruption, no.161 of 19 April 2003, Title III. In: Official Gazette of Romania, no. 279 of 21 April 2003.
2. Council of Europe Convention on Cybercrime. http://www.coe.int/t/dghl/coo peration/economiccrime/cybercrime/Documents/Convention%20and%20proto col/ETS%20185%20Romanian.pdf.
3. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data in Strasbourg on 28 January 1981, ratified by the Republic of Moldova by Decision of the Parliament of the Republic of Moldova No. 483-XIV of 2 July 1999.
4. Law No. 271/2013 regarding the formulation of some declarations of the Republic of Moldova to the Convention for the protection of individuals regarding the automated processing of personal data, published in the Official Gazette of the Republic of Moldova no. 284-289/2013.
5. Law no. 1069/ 2000 on informatics, published in the Official Gazette of the Republic of Moldova no 73-74/2001.
6. Law no. 467/2003 on computerization and state information resources, published in the Official Gazette of the Republic of Moldova no. 6-12/2004.
7. Order no. 18 of 23-01-2001 issued by Ministry of Transport and Communications, published in the Official Gazette of the Republic of Moldova no. 8/2001.
8. Development Strategy for Telecommunications, published in the Official Gazette of the Republic of Moldova no. 218-223/2004.
9. National strategy for the development of the information society "Digital Moldova 202", published in the Official Gazette of the Republic of Moldova no. 252-257/2013.
10. Criminal Code of the Republic of Moldova, No. 985-XV of 18.04.2002, republished in the Official Gazette of the Republic of Moldova no. 72-74/195 of 14.04.2009.

11. Programme for preventing and combating crime for the years 2022 - 2025, https://cancelaria.gov.md/sites/default/files/document/attachments/721.pdf.
12. Recommendation for a Council Decision authorising participation in negotiations on the Second Additional Protocol to the Council of Europe Convention on Cybercrime (CETS No. 185), https://eur-lex.europa.eu/legal-content /RO/ ALL/?uri=CELEX:52019PC0071.

III. Electronic sources

1. *All about hacking*, https://www.britannica.com/topic/cybercrime/Hacking.
2. *EU fight against organised crime*, https://www.consilium.europa.eu/ro/policies/eu-fight-against-crime/.
3. *Cyber security: how the EU is fighting cyber threats*, https:// www.consilium.europa.eu/en/policies/cybersecurity/.
4. *Sixth progress report on achieving a real and effective security union*. European Commission, Brussels from 24.04.2017, www.ipex.eu.
5. *Online Organised Crime Threat Assessment (IOCTA)*, 2016: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threata ssessment-iocta-2016.
6. *Informing citizens about cybercrime and ways to protect personal data and assets*, https://www.mai.gov.md/ro/node/7213.
7. *Better access to electronic evidence to fight cybercrime and related crimes*, https://www.mai.gov.md/ro/node/7359.
8. *Police Activity Report 2022*, https://politia.md/sites/default/files/raport _activity _12_month_2022_.pdf.
9. *National Cyber Security Index*, https://ncsi.ega.ee/compare/.
10. *Brief history of cyber security and hacking*, https://cybernews.com/security/brief-history-of-cybersecurity-and-hacking/.
11. *Who invented viruses. What is a computer virus*, https://2too.ru/ro/programs/kto-izobrel-virusy-chto-takoe-kompyuternyi-virus.html.
12. *Cybercrime*, https://guyanapoliceforce.gy/?page_id=2071.
13. *Identity theft and financial fraud*, https://bjs.ojp.gov/topics/crime/identity-theft.
14. *Spam, steganography and e-mail hacking*, https://www.britannica.com/topic/cybercrime/ Spam-steganography-and-e-mail-hacking.
15. *Texas bank error that exposed thousands of Social Security numbers*, https://cybernews.com/news/happy-state-bank-breach/.
16. *US private university suffered cyberattack*, https://www.Bleeping computer.com/news/security/ransomware-gang-hijacks-university-alert-system-to-issue-threats/.
17. *A U.S. security researcher has discovered a vulnerability accessing Toyota's management system*, https://www.bleepingcomputer.com/news/security/researcher-breaches-toyota-supplier-portal-with-info-on-14-000-partners/.
18. *Cybersecurity News*, https://stisc.gov.md/ro/noutatile-saptamanii-din-cybersecurity-6052022.
19. *Cybercrime Investigations Report*, Verizon 2022, https://www.verizon.com/business/resources/reports/dbir/2022.
20. *Latest Cybercrime Statistics*, https://aag-it.com/the-latest-cyber-crime-statisti

cs/.
21. *Most Common Cybercrimes*, https://www.enkanter.com/article/9-most-common-computer-and-internet-cyber-crimes.
22. *DDoS attack scheme*, https://bunny.net/academy/network/what-are-distributed-denial-of-service-ddos-attacks.
23. *Moldova's ranking according to NCSI*, https://ncsi.ega.ee/compare/.
24. *Most types of cybercrime reported worldwide in 2022, by number of people affected*, https://www.statista.com/statistics/184083/commonly-reported-types-of-cyber-crime-global/.
25. *IC3: Total damage caused by reported cybercrime 2001-2022*, https://www.statista.com/statistics/267132/total-damage-caused-by-by-cyber-crime-in-the-us/.
26. *Percentage of internet users in selected countries who have ever suffered a cybercrime, November-December 2022*, https://www.statista.com/statistics/194133/cybercrime-rate-in-selected-countries/.
27. *Evolution of malware attacks from 1984 to 2018*, https://www.av-test.org /en /statistics/malware/.
28. *Distribution of cyber attacks in industries worldwide in 2022*, https://www.statista.com/statistics/1315805/cyber-attacks-top-industries-worldwide/.
29. *Countries with the most significant cyber attacks, 2006-2020*, https://specopssoft.com/blog/countries-experiencing-significant-cyber-attacks/.
30. *Mafia Boys computer crime*, https://www.wired.com/2007/02/feb-7-2000-mafia boys-moment-2/.
31. *March 2023 broke ransomware attack records with 459 incidents*, https://www.bleepingcomputer.com/news/security/march-2023-broke-ransomware-attack-records-with-459-incidents/.
32. *Record number of ransomware attacks in March 2023, according to a report released by NCC Group*, https://www.bleepingcomputer.com/news/security/march-2023-broke-ransom ware -attack-records-with-459-incidents/.