International Journal Of Law And Criminology
(ISSN – 2771-2214)
VOLUME 04 ISSUE 02 PAGES: 116-120
SJIF IMPACT FACTOR (2021: 5. 705) (2022: 5. 705) (2023: 6. 584)
OCLC – 1121105677
Crossref doi Google Scholar WorldCat MENDELEY
Publisher: Oscar Publishing Services

Journal Website: https://theusajournals.com/index.php/ijlc

Research Article

GENESIS OF CYBERCRIME AND ITS CONCEPT PECULIARITIES

Submission Date: February 18, 2024, Accepted Date: February 23, 2024,
Published Date: February 28, 2024
Crossref doi: https://doi.org/10.37547/ijlc/Volume04Issue02-20

Aybek Orazbayevich Khalmuratov
Senior Lecturer Of The Department Of Criminal Law And Criminology Of The Law Enforcement Academy Of The Republic Of Uzbekistan

ABSTRACT

The article deals with the history of the origin of cybercrime. It describes in detail the essence and peculiarities of cybercrime terminology. At the same time, the article reveals types of cybercrime, as well as its goals and objects of influence.

KEYWORDS

Cybersecurity, cybercrime, cyberspace, Internet, cyberattack.

INTRODUCTION

In today's world, 54% of the total population of planet Earth actively use digital gadgets [1], and the number of people using personal computers reaches approximately 370 million people, a relatively young, yet very dangerous type of crime called cybercrime is gaining popularity.

Cybercrime is a type of act recognized as criminal, where the subject commits a cyberattack for various motives and purposes. Moreover, the subjects of this type of crime are cybercriminals who carry out the subjective side of the crime through technological means, attempting to personal data, various kinds of information, as well as finances, etc.

Considering the genesis of cybercrime, it is logical to believe that this type of crime emerged with the spread of the Internet. The etymology of the word "cybercrime" comes from the English words "cyber" + "crime". It is necessary to distinguish the concept of computer crime from cybercrime, as the latter is more extensive and involves the commission of criminal acts in cyberspace, using not only computers, but also other information and communication technologies, the Internet and other digital networks. It is known that the first information network, named "ARPANET", was created in 1969 in the United States, with exclusively political purposes at the height of the "Cold War" [2]. Further, with the spread and development of the

International Journal Of Law And Criminology
(ISSN – 2771-2214)
VOLUME 04 ISSUE 02 PAGES: 116-120
SJIF IMPACT FACTOR (2021: 5. 705) (2022: 5. 705) (2023: 6. 584)
OCLC – 1121105677
Crossref doi Google Scholar WorldCat MENDELEY
Publisher: Oscar Publishing Services

World Wide Web, when ordinary citizens could access the Internet, the first cases of fraud, namely cyberfraud, were born. Thus, for example, in the late 1980s, the first powerful wave of cybercrime occurred, when by sending malicious programs through e-mail, cyberfraudsters gained access to personal data of users, which contributed to the commission of various money scams and financial pyramids. This type of cybercrime is currently referred to as Phishing.

The first international treaty that regulated crimes committed in cyberspace, in particular those related to computer fraud, copyright infringement, distribution and storage of child pornography and breach of network security, is the Budapest Convention, adopted on November 23, 2001 [3].

Among the types of cybercrime, the following are distinguished:

I. Fraud through the use of the Internet and e-mail.

II. Theft, theft of digital and financial information, personal data, and payment card data. Cybercrime can have serious consequences for individuals, organizations, and governments, including leakage of confidential information, financial loss, and breach of privacy.

III. Cyber blackmail, i.e. extorting money from (target) a person or access to obtain their finances under the threat of a cyber attack.

IV. Cyber espionage, i.e. illegal attempt, to gain access to data of government agencies and other corporate organizations. Cybercrime can also be used to carry out espionage, cyberterrorism and other forms of cyber-attacks.

V. Online trade in illicit goods - the process of online purchase, sale and distribution of illicit narcotic drugs, psychotropic substances, precursors, as well as pyrotechnics, edged weapons and so on.

IV. Cyber espionage is the illegal targeting, gaining access to data of government agencies and other corporate organizations. Cybercrime can also be used to carry out espionage, cyberterrorism and other forms of cyber-attacks.

V. Online trade in illicit goods - the process of online purchase, sale and distribution of illicit narcotic drugs, psychotropic substances, precursors, as well as pyrotechnics, edged weapons and so on.

VI. Cyberattacks on infrastructure - cybercriminals can target critical infrastructure such as energy systems, transportation networks and communication systems to damage the economy and society.

Next, it should be established what can be targeted by cybercrime, or more specifically, what is being targeted. These include:

– computer crimes that infringe on state and public interests;

– cybercrimes that infringe on personal rights and privacy;

– economic cybercrime, which attacks the finances of individuals (natural and legal) persons.

Cybercrime always implies intent, followed by action (a cybercrime act cannot be expressed in inaction), consequence and a causal link between them. The goals of cybercrime acts can actually be generalized into the four categories listed below. However, the public danger arising from them is of a serious nature and is capable of inflicting great material property and non-property, as well as physical and moral damage.

International Journal Of Law And Criminology
(ISSN – 2771-2214)
VOLUME 04 ISSUE 02 PAGES: 116-120
SJIF IMPACT FACTOR (2021: 5. 705) (2022: 5. 705) (2023: 6. 584)
OCLC – 1121105677
Crossref doi Google Scholar WorldCat MENDELEY
Publisher: Oscar Publishing Services

Cybercrime is a threat to the global economy, causing billions of dollars in damage every year.

Let us list the types of targets and give a concept for each of them:

Economic – based on illegal enrichment. They are one of the most common targets of Internet fraudsters. It manifests itself in the withdrawal of money from bank cards; organization of pseudo-money collections, allegedly directed to the treatment of sick children or animals, extortion of various sums of money, due to the mastery of private information, etc.

Ideological – based on the dissemination of extremist and terrorist recruitment and various kinds of calls to commit socially dangerous acts, such as terrorist attacks and inter-religious wars.

Political – aimed at destroying the current domestic policy and the constitutional order of the state.

Social-psychological – aimed at leading or inducing persons to commit suicide, as well as to lure persons into deviant groups and to commit various kinds of antisocial socially dangerous acts.

Let's take a look at a small list of common types of cyberattacks that can be used by cybercriminals to harm computers, networks and data.

Malware attacks – viruses, worms, Trojan horses, and other malicious programs that can infect computers and networks, harbor data, or cause other damage.

DDoS attacks – denial of service cyberattacks in which attackers overwhelm a network or server with traffic to temporarily or permanently stop access to resources.

Ransomware – cyberattacks in which attackers encrypt data or block access to a system and demand a ransom to restore it.

Social engineering – cyberattacks in which attackers use manipulation and deception to gain access to sensitive information or systems.

SQL injection – cyberattacks on websites in which attackers inject SQL code into database queries to gain unauthorized access to data.

File attacks – using malicious files, such as executable files or documents with macros, to infect computers.

Software vulnerability cyberattacks – exploiting known vulnerabilities in software to gain unauthorized access to a system or data.

Combating cybercrime requires a joint effort of the international community, individual countries, legal entities and individuals, as well as the development of new technologies and methods of information protection. There are a number of ways to combat cybercrime in developed countries, including:

First, establishing strong legislative measures, as well as strict laws and regulations that establish accountability for cybercrime and provide penalties for cyber offenders. Second, cooperation between law enforcement and the private sector, i.e., developing partnerships between law enforcement, business companies and government organizations to share information about cyber threats and jointly combat them.

Next, the level of cybersecurity in the country, which is achieved through the implementation of technical means of information protection, in addition, the training of personnel in the field of cybersecurity and,

International Journal Of Law And Criminology
(ISSN – 2771-2214)
VOLUME 04 ISSUE 02 PAGES: 116-120
SJIF IMPACT FACTOR (2021: 5. 705) (2022: 5. 705) (2023: 6. 584)
OCLC – 1121105677
Publisher: Oscar Publishing Services

last but not least, the development of strategies to prevent cyberattacks.

Hence, international cooperation, which means the state's participation in international organizations aimed at combating cybercrime, exchange of information and experience with other states.

Another important aspect is improving the level of education and training of citizens in this area, conducting educational programs to raise awareness of cyber threats among the population, the business community and government agencies.

And of course, developing new technologies, finding innovative methods and ways to prevent, prevent and combat cybercrime. And also, investing in research and development of new technologies to detect cyberattacks.

CONCLUSION

In conclusion, it should be noted that hacker hooliganism, which used to be seemingly ordinary at first glance, has grown into a serious type of crime in the 21st century, which is gaining momentum and every year entails more and more unpleasant consequences for the targets of cybercriminals. Each state should take this type of crime seriously, recognize it as a criminal offense, keep records and statistics, carry out various activities to prevent and suppress such acts, as well as to improve performance in combating cybercrime should introduce new techniques and technologies and cooperate with other countries to share experience and information.

Thus, we can take the example of influential personalities who recognize the real threat of cybersecurity in today's world. One of them is B. Obama, who stated that "The virtual threat is one of the most serious security and economic challenges we face. And US Director of National Intelligence James Clapper stated that "In a virtual environment, technology advances and is deployed faster than security measures are prepared". Offensive actions are achieved quickly, while network defenses improve much more slowly [4].

That is why cybersecurity is very important and has a place in every developed nation. Microsoft Corporation has developed publicly available cybersecurity guidelines and solutions, among which are listed:

– credential protection;

– threat detection and prevention;

– data protection and individual e-cloud protection [5].

Adherence to the above tips is becoming an integral part of a network cybersecurity strategy for both individuals and organizations that seek to provide robust protection against network threats and cyberattacks.

REFERENCES

1. Smartphone Owners Are Now The Global Majority, New Gsma Report Reveals URL: https://www.gsma.com
2. Volevodz A.G. - Countering cybercrime - the topic of the first thematic issue of the publication "Library of Criminalist. Scientific Journal". №5 (10)-2013 y.
3. Budapest Convention URL: https://www.coe.int/ru/web/impact-convention-human-rights/convention-on-cybercrime.
4. Starkin S.V. – "Cyber security and cyber revolution: critical analysis of basic concepts". Paper. Moscow State University. Ser. 12. Political Science. 2015 y. №1.

International Journal Of Law And Criminology
(ISSN – 2771-2214)
VOLUME 04 ISSUE 02 PAGES: 116-120
SJIF IMPACT FACTOR (2021: 5. 705) (2022: 5. 705) (2023: 6. 584)
OCLC – 1121105677
Publisher: Oscar Publishing Services

5. Microsoft Security "What is Cybersecurity?" URL: www.microsoft.com