E-ISSN: 2997-9439

American Journal of Education and Evaluation Studies

https://semantjournals.org/index.php/ AJEES

| Research Article

Check for updates

Types of Cybercrimes and Possibilities for International Cooperation in their Analysis and Collection of Digital Evidence

Normurodova Behroza Kholmominovna

Lecturer, Department of Cyber Law, Tashkent State University of Law

Nbdjsinger@gmail.com

Abstract: This article provides information about cybercrimes, their types, the history of their emergence and development. First of all, it explains what crimes are understood as cybercrimes, their classification into types, and qualifications. In addition, the reasons for the increase in cybercrimes in the current digital world and the measures that should be taken to combat them are discussed. The reasons for the commission of cybercrimes, the gaps in the security system that pave the way for them are indicated, the issue of liability for cybercrimes, and the current situation related to this topic are discussed. At the same time, proposals for legislation to improve the current situation, prevent cybercrimes, and establish liability for them are presented.

Keywords: cybercrime, Internet fraud, personal information, cyberattacks, hacking, virus, malware, forensics, digital evidence.

1. Introduction

Cybercrime is the illegal use or attack of digital devices and networks by hackers or other criminals. Some cybercriminals are technically very skilled and use well-organized and sophisticated methods. Threats to the financial or political security of a country or cyberterrorism are examples of cybercrime, which involves economic, personal, and political attacks on computers.

Cybercrime is the use of digital devices as a tool for illegal purposes, such as fraud, child pornography and intellectual property trafficking, identity theft, or invasion of privacy.

Nowadays, there are many types of cybercrimes. As digital devices and programs develop year after year and their types increase, the types of cybercrimes are also increasing. In particular, we are witnessing the fact that countries in a state of war in the world are launching cyberattacks on each other. In this situation, first of all, ensuring cybersecurity, preventing cybercrimes and determining responsibility for them are becoming the main goals. This article studies issues such as cybercrimes, their types, their analysis, determining responsibility for them, and based on the information provided, proposals are made for legislation.

2. Methodology

This article examines the gaps in the legislation related to cybercrimes, their types, their qualification, cybercrimes and the establishment of responsibility for them, and presents alternative solutions to existing problems. The commission of cybercrimes has increased in the Republic of Uzbekistan in recent years. Since cybercrimes are a new type of crime for us, their analysis, their types and responsibility, issues related to investigation and collection of digital evidence are not fully reflected in the legislation. Therefore, first of all, it is important to study the experience of advanced foreign countries in this area.

This article uses the copying method. That is, issues such as information related to cybercrimes, cases of cybercrimes, their detection and investigation, and determination of responsibility are studied based on the experience of foreign countries. The advantage of studying foreign experience is that we can eliminate the shortcomings in them by getting acquainted with the practice. In addition, scientific articles, cases, manuals, and regulatory legal documents related to cybercrimes are collected and their analysis is presented in the article. At the same time, limitations related to the study of cybercrimes, gaps in the legislation, and existing problems in the current state are indicated and solutions are provided to them. Also, proposals for legislation to solve these problems are made.

3. Results

In 1996 The Council of Europe, together with representatives of the governments of the United States, Canada, and Japan, drafted the first international treaty covering cybercrime.[1] Civil libertarian groups around the world immediately objected to the treaty's provisions requiring Internet service providers (ISPs) to store data on their customers' transactions and to hand over this information upon request. Work on the treaty continued nonetheless, and on 23 November 2001, the Council of Europe Convention on Cybercrime (Budapest Convention) was signed by 30 states. The convention entered into force in 2004. Additional protocols covering terrorist activities, racist and xenophobic cybercrime were proposed in 2002 and entered into force in 2006.[2] Additionally, the USA PATRIOT Act of 2001 expanded the law, giving law enforcement authorities the authority to monitor and protect computer networks.[3]

In 2015 The U.S. Bureau of Justice Statistics (BJS) has released a report on identity theft. According to it, in 2014, almost 1.1 million Americans had their personal information fraudulently used to open bank, credit card, or utility accounts. The BJS report found that the total number of identity theft victims in the United States has increased by approximately 1 million since 2012, with total losses to individuals reaching $15.4 billion since 2012.[4]

4. Discussion

NewWhile technology has provided many conveniences to every industry, it has also created new criminal opportunities. How is cybercrime different from traditional criminal activity? One difference is undoubtedly the use of digital devices, but technology alone is not enough to account for any differences that may exist between different areas of criminal activity. Criminals do not need a digital device to commit fraud, child pornography and intellectual property trafficking, steal personal information, or violate someone’s privacy. All of these activities existed before the “cyber” prefix became ubiquitous. Cybercrime, especially those related to the Internet, refers to the expansion of existing criminal behavior along with some new illegal activities.

Most cybercrimes involve attacks on information about individuals, corporations, or governments. While the attacks do not occur in a physical environment, they occur in a personal or corporate virtual environment, which is a collection of information attributes that identify people and institutions on the Internet. In other words, in the digital age, our virtual identities are essential elements of everyday life. We are a collection of numbers and identifiers in multiple computer

databases owned by governments and corporations. Cybercrime demonstrates the centrality of networked digital devices in our lives, and the insecurity of seemingly reliable facts such as personal identities.

A significant aspect of cybercrime is its transboundary nature, meaning that acts can occur in jurisdictions separated by vast distances. This poses significant challenges for law enforcement, as crimes that were once local or national now require international cooperation. For example, if a person accesses child pornography material on a computer in a country where child pornography is not prohibited, will that person be considered to have committed a crime in a country where such material is illegal?

Where exactly does cybercrime occur? As a global network, the Internet offers criminals several hiding places, both in the real world and on the Internet itself. However, just as people who walk on land leave footprints, cybercriminals leave traces of their identity and location, despite their best efforts to hide their tracks. Such traces are called "artifacts."

Below are the reasons why cybercrimes are committed:

- Vulnerable devices. As we mentioned above, the lack of effective security measures has led to the existence of a wide range of vulnerable devices that are easy targets for cybercriminals;
- Personal motivation. Cybercriminals sometimes commit cybercrimes to get revenge on someone they hate or have a problem with;
- Financial motivation. The most common motivation of cybercriminals and hacking groups, with most attacks today aimed at financial gain.
- Political goals;
- Implementing terrorist ideas.[5]

Types of cybercrime

Cybercrime encompasses a wide range of activities and is considered a crime that involves a fundamental breach of personal or corporate privacy, such as the violation of the integrity of data stored on digital devices and the use of illegally obtained digital data to harass, harm, or blackmail a company or individual.

VariousCompanies are installing spyware on digital devices that track the location of the device and the identity of the device's owner. The companies have said that these programs are only used to prevent crime and track criminals. However, spyware attached to smartphones, which can steal personal information, has been widely used by governments to secretly monitor politicians, government leaders, human rights activists, dissidents and journalists.

The US Department of Justice (DOJ) divides cybercrime into the following three categories:

- ✓ Crimes where a computing device is targeted -- for example, to gain access to a network.
- ✓ Crimes in which a computer is used as a weapon -- for example, to launch a denial of service (DoS) attack.
- ✓ Crimes in which a computer is used as an accessory to a crime -- for example, using a computer to store illegally obtained information.[6]

There are many types of cybercrime. As digital devices and programs develop, their types are also increasing. Below you can learn about the most common types of cybercrime and the methods by which they are committed.

Internet fraud

There are many ways to deceive consumers online. One of them is Internet fraud. Internet fraud involves the use of online services and programs that have access to the Internet to deceive or exploit victims. The term "Internet fraud" generally refers to cybercriminal activities that occur over the Internet or via email, including identity theft, "phishing," and hacking activities designed to extort money from people. Millions of dollars are lost each year due to Internet fraud that targets victims through online services. These numbers are increasing as Internet use expands and cybercrime techniques become more sophisticated. There are several types of Internet fraud, including:

- "Phishing" and fraud: The use of email and online messaging services to trick victims into sharing personal information, login credentials, and financial information.
- Data Breach: The theft of confidential, protected data from a secure location and its transfer to an untrusted environment. This includes data stolen from users and organizations.
- Denial of Service (DoS): Interrupting traffic access to an online service, system, or network in order to commit a crime.
- Malware: The use of malicious software to damage users' devices, delete data, or steal them.
- Ransomware: A type of malware that blocks users from accessing important data, then demands a ransom with the promise of restoring access. Ransomware is typically delivered through "phishing" attacks.
- Business Email Compromise (BEC): A sophisticated form of attack targeting businesses that frequently make money transfers. It compromises legitimate email accounts through social engineering techniques to send unauthorized payments.[7]

ATM fraud

Over the past few decades, automated teller machines (ATMs) have become commonplace in everything from bank lobbies to shopping malls, from gas stations to bus and subway stations. As of 2022, there are over 2.2 million ATMs worldwide.[8] Their ubiquity has led people to use these virtual cash dispensers without hesitation. The thought that something could go wrong never even occurs to them. In 2002, the New York Times reported that more than 21,000 bank accounts had been compromised by a group that was illegally obtaining ATM data.[9] A particularly effective form of fraud involves the use of ATMs in shopping malls and stores. Criminals can easily set up a machine that looks like a legitimate machine. Instead of dispensing money, this machine collects information about users and only shows that it is malfunctioning after they enter their PIN. Considering that ATMs are the most common way to dispense currency worldwide, ATM fraud has become an international problem.

ATMThere are several types of fraud, including:

- "Card skimming" is a popular type of fraud. In this case, a hidden device is installed in an ATM, which allows it to read information from payment cards during ATM transactions. As a result, criminals create a duplicate card with a PIN code written on the magnetic strip. The duplicate card allows criminals to make payments at various points of sale.
- A "card trap" is a device placed in an ATM card reader that prevents the cardholder from removing the card after the machine has completed a transaction. The fraudster typically captures the PIN number through a hidden video camera built into the ATM's panel. If the customer leaves without removing the card, the fraudster removes the payment instrument and then uses someone else's card to make payments or withdraw cash.

- "Jamming of keyboard." In this, fraudsters block important keys (Cancel, Enter, etc.) on the ATM keyboard to prevent a successful transaction. Then, once the required information is entered, the criminal uses the ATM to withdraw cash.
- "Phishing." "Phishing" refers to the theft of card information from a cardholder. This type of fraud involves the theft of passwords, credit card numbers, bank account numbers, and other confidential information. Cybercriminals use personal information to gain access to accounts linked to bank cards, allowing them to steal money from card accounts.
- SMS fraud. In this method, an SMS message is sent to the user. The purpose of such a message is to force the person to give the fraudster their card details. The message may contain information about blocking the card. In order to unblock it, the fraudster may request the card details. Another method is to send a message to a relative or friend of the cardholder that the user's life is in danger. In this case, the fraudster can get both money and card details.[10]

File sharing and piracy

1990sDuring the 1990s, sales of compact discs (CDs) were the main source of revenue for record companies. Although piracy, the illegal copying of copyrighted material, had always been a problem, especially in the Far East, the proliferation of inexpensive personal computers on college campuses that could rip music from CDs and share them at high speed ("broadband") Internet access became the biggest threat to the recording industry. In the United States, the recording industry, represented by the Recording Industry Association of America (RIAA), attacked Napster, the only file-sharing service that allowed users to access music files stored on data over the Internet, from 1999 to 2001. The files, known as MP3s, were stolen from other users' computers via Napster's central computer.[11]

"Cyberbullying"

Cyberbullying is bullying that occurs on digital devices such as mobile phones, computers and tablets. Cyberbullying can occur via text messages, apps or online on social media, forums or games where people can view, participate in or share content. Cyberbullying is the sending, posting or sharing of negative, harmful, false or abusive content about another person. Cyberbullying is most commonly committed on social media such as Facebook, Instagram, Snapchat and Tik Tok, text messaging apps on mobile or tablet devices, instant messaging, direct messaging and online chat, online forums, email, etc.[12]

Cybstalking

"Cyberstalking" -Stalking through websites, search engines, and social media.[13] This crime can usually be committed through a person's social media pages, email addresses, and private correspondence, as well as through very dangerous stalking programs.[14] For example, "key logging" programs. This is one of the most powerful stalking programs. That is, it allows you to track all correspondences made on the device on which this program is installed, search commands given to applications, in short, all records online.

Cyberterrorism

Cyberterrorism is the use of the Internet to incite acts of violence that threaten to achieve political or ideological gains through threats or intimidation. The deliberate, large-scale disruption of computer networks, particularly digital devices connected to the Internet, using tools such as computer viruses, computer worms, phishing, malware, and programming scripts can be forms of cyberterrorism.

Child pornography

Child pornography is the crime of distributing images, pictures, or videos of minors engaging in sexual activity online. 98.9% of perpetrators are male, with an average age of 41. In the United States, there were 1,435 reported cases of child pornography in 2022, and 98.7% of those convicted were sentenced to prison.[15]

Hacking

Hacking is the act of finding vulnerabilities in a system and stealing confidential information from there. Not all types of hacking are bad. People who find and exploit security flaws in systems are also a type of hacker and are called “white hat hackers.” “Black hat hackers” are the same type of hackers we usually know.[16]

Hacking can be done through various methods:

- Social engineering is a manipulation technique designed to exploit human error to gain access to personal information. Hackers can trick you into revealing personal or financial information by using fake identities and various psychological tricks. To achieve this, they may rely on "phishing" scams, spam emails or instant messages, and even fake websites.
- Password cracking. Hackers use a variety of methods to obtain passwords. In this method, hackers can try to guess all possible password combinations to get in. Hackers can also use simple algorithms to generate different combinations of letters, numbers, and symbols to help them figure out password combinations. Another method is known as a dictionary attack, which allows the program to enter common words into password fields and see if any of them work.
- Malware-infected devices. Hackers can infiltrate a user's device to install malware. They can target potential victims through email, instant messaging, and websites or networks with downloadable content, applications, and programs.
- Using unsecured wireless networks. Instead of using malicious code to access someone else's computer, hackers can use open wireless networks (such as Wi-Fi routers). Not everyone secures their router, and this can be exploited by hackers looking for an open, secure wireless connection. This is an activity known as scanning for wireless networks. Once hackers connect to an unsecured network, they only need to bypass basic security to gain access to devices connected to that network.
- Email Spying. Hackers can create code that allows them to intercept and read email messages. Most email programs today use encryption formulas, meaning that even if hackers intercept the message, they cannot read it.
- Key logging. These programs allow hackers to track every keystroke a computer user makes. Once installed on a victim's computer, the programs record every keystroke, giving the hacker everything they need to break into the system or steal someone's personal information.
- Creating zombie computers. A zombie computer, or bot, is a computer that a hacker can use to send spam or launch distributed denial-of-service (DDoS) attacks. After the victim performs the specified actions, a connection is opened between their computer and the hacker's system. The hacker can then secretly control the victim's computer, using it to commit crimes or distribute spam.[17]
- "Mirror" sites. In this case, hackers create a copy of legitimate official sites. The user, thinking that this site is a legitimate site, provides the requested information. For example, login, password, passport data, plastic card numbers, etc. Thus, through these sites, hackers can obtain all the user's personal information. In order not to become a victim of this crime, the user should check the officiality and reliability of the site.

Viruses and malware

"Virus"The terms "malware" and "malware" are often used interchangeably, but they are not the same thing. While a computer virus is a type of malicious software, not all malware is a computer virus.[18] A computer virus is a malicious piece of computer code that is designed to spread from device to device. Viruses can typically damage a device, disabling some or all of its systems. Malware can steal, modify, delete, or block data on a device.

Email-related crimes

Email is one of the most common forms of online communication worldwide. Therefore, email is one of the most convenient tools for committing crimes. Crimes related to email include:

1. Email spoofing;
2. Sending malicious codes via email;
3. Email "bombing";
4. Sending threatening emails;
5. Dissemination of defamatory messages via email;
6. Email scams.

Using customer service

Another popular method hackers use to get into your computer is to impersonate Microsoft or Amazon customer support. These scammers pretend to be legitimate and tell you that in order to fix a technical issue, the victim needs to download a remote access program called “AnyDesk.” Once the victim downloads this software and grants the scammer remote access to the computer, the scammer blacks out the victim’s screen so they can’t see what the scammer is doing. The scammer then goes through the computer and downloads the victim’s files, as well as accesses banking apps or websites to see if the victim is logged in. If the victim is logged in, the hackers start withdrawing money from the victim’s account.

Botnets

Botnet -This is a type of cybercrime in which a criminal takes over several computers and combines them to carry out criminal activities. In botnets, criminals can connect to hundreds or even millions of devices, which makes it difficult to stop these crimes. That is, in this case, the location of the devices in the botnet can indicate different countries. In this case, checking all the specified addresses takes a lot of time. During this time, the criminal will have achieved his goal. That is why this crime is considered the most dangerous cybercrime.

5. Conclusion

This article discusses the concept of cybercrimes, their analysis, types, methods of commission, and the issues of responsibility assigned to them. The number of cybercrimes is increasing as the digital world develops. Today, due to the high need for digital devices and programs, and the fact that part of people's lives has moved to the digital world, it is becoming more convenient to commit cybercrimes. The main goal of governments and law enforcement agencies is to develop regulatory and legal documents related to cybercrimes being committed, eliminate gaps in the legislation, prevent new cybercrimes that may arise in practice and ensure the establishment of responsibility for them, and raise awareness among citizens by familiarizing the population with the types of cybercrimes and methods of committing them.

Cybercrimes are considered a new type of crime in the Republic of Uzbekistan, and the criminal legislation does not fully cover these crimes. First of all, it is necessary to include the most common main types of cybercrimes in the Criminal Code and establish liability for them.

There is no specific regulatory legal act in the Republic of Uzbekistan on the investigation of cybercrimes and the identification of criminals. There is a huge gap in this area in the Criminal Procedure Code, and to fill this gap, first of all, digital evidence should be given the status of independent evidence. Cybercrimes differ from other crimes in their characteristics. Therefore, their investigation should also be different from that of ordinary crimes. Studying the experience of foreign countries in investigating cybercrimes, including them in the Criminal Procedure Code, and ratifying international conventions and treaties in this area can help solve existing problems.

References

1. "Cybercrime" by Michael Aaron Dennis. Available at:https://www.britannica.com/topic/cybercrime;
2. Convention on Cybercrime. Budapest, 23.11.2001. Available at:https://rm.coe.int/1680081561;
3. The USA PATRIOT Act: Preserving Life and Liberty 10/25/01. Available at:https://www.justice.gov/archive/ll/what_is_the_patriot_act.pdf;
4. "Federal Justice Statistics, 2015 - Statistical Tables" Mark A. Motivans, PhD, BJS Statistician December 2020. Available at:https://bjs.ojp.gov/library/publications/federal-justice-statistics;
5. What is Cybercrime? Types, Examples, and Prevention. Available at:https://cybertalents.com/blog/what-is-cyber-crime-types-examples-and-prevention;
6. Eshonkulov J. (2025). The Role of Smart Contracts in Civil Law and Issues of Legal Regulation. Uzbek Journal of Law and Digital Policy, 3(1), 104–111. https://doi.org/10.59022/ujldp.294
7. Kate Brush, Michael Cobb. "What is cybercrime?". Available at:https://www.techtarget.com/searchsecurity/definition/cybercrime;
8. Internet Fraud.https://www.fortinet.com/resources/cyberglossary/internet-fraud;
9. LENNY LUBITZ "5 ATM Scams That Can Break the Bank" December 23, 2023. Available at:https://www.investopedia.com/articles/pf/08/avoid-atm-scams-atm-fraud;
10. Eshonkulov, J. (2024). Legal foundations for the application of artificial intelligence Technologies in the Sports Industry. American Journal of Education and Evaluation Studies, 1(7), 240-247. https://semantjournals.org/index.php/AJEES/article/view/320/287
11. Technology Briefing | Internet: SEC Issues Warning On Fraud. Available at:https://www.nytimes.com/2002/06/26/business/technology-briefing-internet-sec-issues-warning-on-fraud;
12. What is ATM fraud: types and cases of ATM scam. 2022-04-26. Available at:https://atmeye.com/blog/what-is-atm-fraud/;
13. "Pro-Napster Protesters Vandalize Web Sites". Mike Ingram. Available at:https://www.wsws.org/en/articles/2000/08/naps-a17;
14. What Is Cyberbullying. Available at:https://www.stopbullying.gov/cyberbullying/what-is-it;
15. "Cybercrime". Available at:https://www.imperva.com/learn/application-security/cybercrime/;
16. Sherry Gordon, Cyberstalking: Definition, Signs, Examples, and Prevention. March 29, 2023. Available at:https://www.verywellmind.com/what-is-cyberstalking-5181466;
17. CHILD PORNOGRAPHY. June 2023. Available at:https://www.ussc.gov/sites/default/files/pdf/research-and-publications/quick-facts/Child_Pornography_FY22;

18. "What is hacking? World-recognized hackers" Muallim Said. Jan 6, 2021. Available at:https://saidakhrorkhonabdukodirov.medium.com/;
19. What is computer piracy? And how to avoid it. Available at:https://www.kaspersky.com.tr/resource-center/definitions/what-is-hacking;
20. What is a computer virus? Available at:https://www.malwarebytes.com/computer-virus;
21. "Email related crime", Tarsem. Available at:https://www.streetdirectory.com/travel_guide/114331;
22. What is a DDoS botnet?. Available at:https://www.cloudflare.com/learning/ddos/what-is-a-ddos-botnet/.