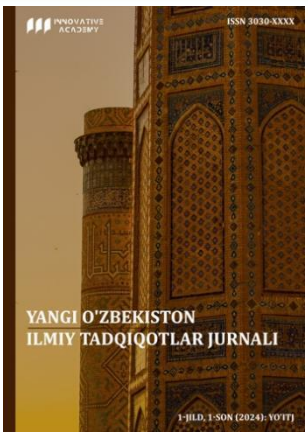

CYBERCRIMES AND CYBER LAW VIOLATIONS: THE DIFFERENCE BETWEEN CRIME AND LAW VIOLATION

Tulkinova Visola Ulugbek kizi
Tashkent State University of Law
Faculty of Criminal Justice Student
Email: visolatolqinova05@gmail.com
https://doi.org/10.5281/zenodo.15517049

ARTICLE INFO

Qabul qilindi:16-may 2025 yil
Ma'qullandi:18-may 2025 yil
Nashr qilindi: 26-may 2025 yil

KEY WORDS

cybercrimes, crime, law violation, phishing, cybersecurity, global network, spam, cyberbullying, cyberterror.

ABSTRACT

This article analyzes the current relevant cybercrimes based on national and international legal norms. The main differences and similarities between crime and law violations are examined. Additionally, advice is provided on preventing cybercrimes that are widespread among the public.

Introduction

Today, as world civilizations develop and countries modernize, entirely new types of crimes and law violations are emerging. The 21st century, as its name suggests, is the era of technology. As the global internet network develops, its vast capabilities are not only creating unprecedented convenience for humanity but are also becoming a source of danger - this is the reality. Cybercrime, with its ever-new types, has entered the list of global problems of our century. We cannot ignore that it poses a great threat to human life through spreading virus software, breaking passwords, stealing funds from credit cards and other bank accounts, and spreading illegal information on the internet, particularly slander and morally corrupt content. Furthermore, the rapid development of computer tools, internet networks, and information technologies, along with the creation of new types, allows users to send or receive any information in text form, audio, or video with just the click of a button. Of course, such conveniences bring people closer together and serve as the most convenient tool for saving time. But have you ever thought about how safely information is being exchanged or how safely information reaches another person? We can find the answer to this question in cybersecurity. The concept of "cybercrime" is explained as terrorism in virtual networks using information and communication technology tools, preparing and spreading viruses and other malicious software, illegal information, mass distribution of electronic messages (spam), hacking attacks, illegal access to websites, fraud, violating data integrity and copyright, stealing credit card numbers and bank account details (phishing and farming) and various other law violations. By 2024, financial losses from cybercrime reached almost 70%. According to Juniper Research researchers, damage increases by an average of 11% annually and exceeded $5 trillion by 2024. Last year, experts estimated damage from cybercrime at $3 trillion.[1] Cybercrimes are the most dangerous form of cyber law violations.

Table of Contents

[1] https://csec.uz/uz/

2. Concepts of cybercrime and cyber law and their history of origin
3. Differences between crime and law violation
4. Types of cybercrime
5. International and national legislation systems on cybersecurity
6. Responsibilities established in national legislation for cybercriminals
7. Conclusion. Author's recommendations
8. List of references

Research Methods Used

In this section, I'll describe the research methods I used to write this analytical essay. First, I provided detailed information about how cybercrime and cyber law violations appeared in society and their impact on society. In revealing the concept of cybercrime, I effectively used "statistical analysis" to show who has suffered from these types of crimes and how much they hinder the country's development through "comparative analysis" - through the opinions of scientists and trends and indicators of states.

To further expand this essay, I drew from the opinions of foreign scientists, scientific articles, and speech texts from sessions of certain international organizations. In addition to these, I have informally commented on legal norms and socio-legal changes in some parts of the essay using the **comparative interpretation** and **logical interpretation** methods commonly found in state and legal theory.

Concepts of Cybercrime and Cyber Law, History of Origin

As mentioned above, **Cybercrime** is *a type of crime committed through the combined connection of computer and network.* The computer serves as a targeted weapon during the crime. Cybercrime is committed with the goal of harming someone's security and financial level.

There are many crimes related to cybercrimes that occur when confidential information is legally protected. On an international scale, both government and non-governmental entities are engaged in cybercrimes, including espionage, financial theft, and other cross-border crimes. Cybercrimes that cross international borders and include the actions of at least one nation-state are sometimes called cyberattacks. **Warren Buffett describes cybercrime as "humanity's number one problem" and adds that it "poses a real threat to humanity."**

Although cybercrime is a new concept, it has already entered the economies of many countries. **Cybercrime** is *a type of crime committed through the combined connection of computer and network*. Cybercrime includes any crime that can be committed using information communication technologies in a computer system or network. Currently, there are many types of cybercrimes, and states are developing various mechanisms to eliminate them. Cybercrime is committed with the goal of harming someone's security and financial level. *One such cybercrime was the first "electronic crime" committed in 1971. That year, the US "New York Pennsylvania Central Railroad" railway company discovered that 200 wagons loaded with valuable cargo had gone missing. During the investigation, it was found that wagons from several other firms had also disappeared. Careful investigation revealed that the cause of the missing wagons was the deliberate entry of incorrect addresses into the computer.* **This was the first officially recorded "electronic crime." Former US President Barack Obama, who witnessed such cybercrimes, said: "Cybersecurity is one of the most pressing problems**

of the 21st century. It is no less than nuclear and mass destruction weapons." Today, both computers and communication systems have developed to an unprecedented degree. This has also created new opportunities for "electronic criminals."

It should be noted that the concept of global network crime does not fully match the previously existing concept of ***"computer crime,"*** and therefore this type of crime is now referred to as ***"cybercrime."*** In international scientific and legal practice, initially the term "computer crime" was used, later ***"computer-related crime," "committing crime through computer," "electronic crime" and "high-tech crime," "virtual crime"*** were used, and today the term ***"cybercrime" or "global network crime"*** is applied. The main purpose of creating these concepts was to clearly define the boundaries of crime committed through the global Internet network and to explain that a specific approach is needed to combat it. **I. Toraxodjaeva** emphasizes that ***"cybercrime is considered a broader concept than computer crime."***

The time-related interconnection of the cybercrime concept can be emphasized by the fact that the main features of computer crimes were initially defined based on the technical capabilities of information communication technologies available at that time by the **Dallas Bar Association conference in 1979**. The collection of cybercrimes constitutes cybercrime, and according to **L. Boranov**, **"cybercrime is a collection of crimes that combines many types of crimes in the field of information communication technologies." L. Kochkina** recognizes cybercrime as ***"crimes in the field of computer data," "information crimes," "crimes related to computer equipment," "crimes in high-tech computers," "crimes in the information field."***

Differences Between Crime and Law Violation

Law violation - *a socially dangerous act that is committed by a subject with legal capacity and is contrary to legal norms and causes harm to the individual, property, state and entire society.* By its nature, law violation can be in the form of crime, unlawful action, or disciplinary violation. In many cases, law violation is used synonymously with lawbreaking.

Law violations are usually divided into 4 groups:

1. Disciplinary law violation
2. Civil law violation
3. Administrative law violation
4. Criminal law violation

Disciplinary law violation - *the violation of labor discipline rules and principles of subordination to management that are mandatory in any labor while performing service duties.*

Criminal law violation - *committing a crime, i.e., theft, robbery, murder, resisting internal affairs officers, and others.*

Civil law violation - *causing damage to the person, property of a citizen or organization.*

Administrative law violation - *According to the Administrative Liability Code of the Republic of Uzbekistan, it is understood as an unlawful, guilty (intentional or negligent) act or inaction that violates the rights and freedoms of individuals, citizens, property, state and public order, and the natural environment, for which administrative liability is provided.*

Crime - *a socially dangerous act provided for in criminal law. The question of considering a certain act as a crime is resolved in each state according to its social system, population's*

lifestyle, national characteristics, customs, traditions, and taking into account international legal norms.

According to Article 14 of the Criminal Code of the Republic of Uzbekistan, the concept of crime is defined as follows: *"A guilty socially dangerous act (action or inaction) prohibited by this Code is found to be a crime under threat of punishment."*

An act that causes harm to objects protected by this Code or creates a real danger of causing such harm is found to be a socially dangerous act."

Types of Cybercrime

The current increase in the number of cybercrimes and the rapid change in types of cybercrimes occurring in the virtual world show that the situation is becoming more serious. Below are the most common types of cybercrimes.

Cyberbullying - means spreading or posting insulting messages about a person or group on the internet using information technologies in the virtual world. Cyberbullying is carried out through information-communication channels and means in the information space. This includes sending destructive video materials and messages (usually with obscene words) via email on the Internet, instant messaging programs (like ICQ), social networks, forums, as well as video portals (YouTube, Vimeo, etc.) or mobile phones (for example, through SMS messages or harassing calls).

Cyberterrorism - the implementation of illegal and subversive actions by an individual or group with the goal of creating various fears and panic between any state or society. Cyberterrorism, in general, can be defined as a terrorist act committed through the use of cyberspace or computer resources. Thus, simple propaganda material on the Internet about bomb attacks occurring on holidays can be considered cyberterrorism. There is also hacking activity aimed at individuals and families, organized by groups within networks, collecting necessary information to create fear among people, demonstrate power, destroy people's lives, as well as looting, blackmail, etc.

Cyberterrorist action (cyberattack) - carried out with the help of computers and information communication tools, directly threatening people's lives and health or potentially threatening, causing great damage to material objects or having the beginning or goal of socially dangerous consequences, is a political reason. The attractiveness of using cyberspace for modern terrorists is related to the fact that implementing a cyberattack does not require large financial expenses. According to experts' conclusions, this is being carried out under the guise of helping the development of developing countries, establishing universal democratic principles, influencing citizens' consciousness, subordinating them to their goals through various means. Unfortunately, in this process, attempts to organize cyberattacks and "effectively" use the unparalleled capabilities of the global internet network are increasingly intensifying. New projects are being developed to reduce these actions. The following can be shown as examples of cyberterrorism incidents:

1. The 2015 cyberattack on Ukraine's electrical networks demonstrates the potential for large-scale disruptions.
2. Terrorist groups use digital platforms for propaganda, as seen in Al-Qaeda's "Inspire" magazine.
3. Encrypted communication platforms are crucial for terrorist operations, as confirmed during the planning of the 2015 Paris attacks.

According to **STATIONX** data, the number of cybercrimes is constantly increasing. According to **2024** calculations, the most frequent cybercrimes were attacks on social media platform providers at **37.4%**, which is **18.2% more than in 2023**. However, cyberattacks on financial institutions (banks, personal accounts) have significantly decreased, from **24.9% in 2023 to 9.8% in 2024**.

Cybercrimes and cyber law violations are carried out by fraudsters or masked hackers on the internet. *The most common type of money-making by cybercriminals is blackmail, that is, demanding money using information about individuals.* This situation occurs as follows:

- A person meets another person on the internet, but in reality, the second party is a fraudster trying to deceive the person.
- They have interesting conversations and quickly seem to establish a deep connection with each other.
- They may even have video chats, but the fraudster uses recorded video or finds excuses for not turning on the microphone or webcam.
- As events develop, the relationship may take on a sexual nature. The fraudster tries to convince the victim to send personal photos or recordings showing themselves in uncomfortable situations.
- Once the fraudster obtains this material, they may even send fake similar photos of innocent people and begin blackmail.
- Now the fraudster threatens to expose the compromising material to family members, colleagues, and others, and offers to destroy this material if payment is made.

International and National Legislation Systems on Cybersecurity

To prevent cybercrimes and cyber law violations, many agreements and treaties are being signed by countries. For example, **The Budapest Convention on Cybercrime of November 23, 2001:**

- Recorded measures to be implemented at the national level in the field of computer information;
- Established types of cybercrimes and penalties for committing them;
- Defined certain procedural features of investigative actions, preservation of data during investigation;
- Proposed general principles of international cooperation and mutual assistance in this area.

The Budapest Convention distinguishes the following types of crimes:

- Crimes against the confidentiality, integrity and availability of computer data and systems;
- Computer-related offenses;
- Content-related offenses;
- Offenses related to violations of copyright and related rights.

The Budapest Convention recommended that each participant (party) develop national legislation necessary to establish the powers and procedures provided for in the provisions of

this document and take other measures. This international document emphasized that the parties' establishment of Convention procedures should be carried out based on the relevant conditions and guarantees, ensuring adequate protection of human rights and freedoms, including rights arising from obligations.

The Agreement on Cooperation in Combating Crimes in the Field of Information Technology between the Commonwealth of Independent States (CIS) member states was signed on September 28, 2018.

According to this agreement, the following are recognized as criminal acts in the field of information technology:

a) Disruption of an information (computer) system through destruction, blocking, modification or copying of information, unauthorized access to computer data protected by law; b) Creating, using or distributing malicious software; c) Violation of computer system usage rules by a person authorized to access the computer system, resulting in the destruction, blocking or modification of computer data protected by law, if this action caused serious damage or severe consequences; d) Theft of property related to changing data processed in a computer system, stored on machine carriers or transmitted through data transmission networks, or entering incorrect data into a computer system or unauthorized access to computer data protected by law; e) Distribution of pornographic materials or objects of pornographic nature with images of minors through the "Internet" information-telecommunication network or other electrical communication channels; f) Illegal use of programs for computer systems and databases that are copyright objects, as well as appropriation of copyright if this act caused significant damage; g) Distribution of materials recognized as extremist in the prescribed manner or containing calls to carry out terrorist activities or justify terrorism, using the "Internet" information-telecommunication network or other electrical communication channels.

In the Republic of Uzbekistan, there are also cases of cybercrimes and cyber law violations, and today the number of such crimes is increasing. **It is noted that by November 2023, 5,500 cybercrimes were committed. Of these, 70% are fraud and theft crimes related to bank cards.** To reduce these indicators and prevent such crimes, **the Law "On Cybersecurity" was adopted on April 15, 2022.** In **Article 3** of this law, cybercrime is defined as follows: "**cybercrime** - a collection of crimes carried out using software and technical means in cyberspace for the purpose of acquiring information, changing it, destroying it, or disabling information systems and resources."

Responsibilities Established in National Legislation for Cybercriminals

Additionally, responsibilities are established in the legislation of the Republic of Uzbekistan for persons who commit cybercrimes, including: In the Code of Administrative Liability of the Republic of Uzbekistan (hereinafter referred to as CAL), administrative violations against information security include **violation of information use rules (CAL Article 155), violation of computer system use rules (CAL Article 155(1)), illegal preparation and distribution of mass media products (CAL Article 218).** Administrative violations that can be committed in the information-communication space also include acts committed using mass media, telecommunication networks, or the global Internet network. These include violations provided for in **CAL Articles 189, 189(1), 191**. Violations provided for by these *CAL Articles 189, 189(1), 191 (pornography, gambling, violence, promoting ideas of war and violence in young people's consciousness; promoting narcotics, psychotropic substances) are committed through illegal actions that threaten citizens', including minors', lives and/or health*

or the lives and/or health of other persons. Additionally, administrative liability is established for distributing illegal content on the global Internet network according to **CAL Article 276**.

In Chapter XXI "Crimes in the Field of Information Technology" added to the Criminal Code of the Republic of Uzbekistan, liability is established for the following crimes:

- CC Article 278(1). Violation of informatization rules
- CC Article 278(2). Illegal (unauthorized) use of computer information
- CC Article 278(3). Preparation or transfer and distribution of special means for illegal (unauthorized) use of computer systems, as well as telecommunication networks
- CC Article 278(4). Modification of computer information
- CC Article 278(5). Computer sabotage
- CC Article 278(6). Creating, using or distributing harmful programs.

Conclusion. Author's Recommendations

I would like to provide my personal suggestions for reducing the number of cybercrimes, which are among the most common crimes in our lives today. First, we need to call citizens to vigilance. Because many individuals carelessly entrust their bank account numbers, phone numbers, email addresses, or similar information to other people. One of the common cybercrimes in our lives is fake correspondence or various types of virus files through Telegram messengers. To prevent these, training sessions should be held in every neighborhood to provide detailed information about these crimes, involving experienced specialists in this field. Next, we need to train more specialists in this field and send them to various countries to study cybercrimes, find solutions, and implement them into our legislation.

As technology advances, the number of cybercrimes and cyber law violations will continue to increase if we don't find solutions. Therefore, I believe that the fields of cyber law and cybersecurity should be widely disseminated to society.

The final conclusion is that cybercrime is a widespread dangerous problem. This crime can target anyone, anywhere, at any time. Therefore, we must be careful about our own actions and strengthen information security and the legal system.

BIBLIOGRAPHY:

LEGAL LITERATURE

1. Cyber law as a field of law: treatise / compilers R.R.Shakurov, M.M.Vohidov. - Tashkent: Center for Professional Development of Lawyers under the Ministry of Justice of the Republic of Uzbekistan, 2022. - 27 p.
2. Ilmiytadqiqot.uz.M.S.Berdimurodova: "Internet security and cybercrime in the globalization process". Issue 1. Volume 1. 2022. July.
3. Marcel, Sébastien. Handbook of Biometric The role of information media in cyber security. nti-Spoofing. London. England. 201

SCIENTIFIC ARTICLES AND JOURNALS USED

4. Toraxodjaeva I. Problems of combating crime committed through the Internet network in Uzbekistan // - T.: Bulletin of Legal Sciences / Vestnik yuridicheskix nauk / Review of law sciences. - scientific-practical journal. 2019 (03) issue. - P.128-132.
5. Shirokov V.A., Bespalova E.V. Cybercrime: history of criminal law counteraction. - M.: "Information Law", 2006. № 4. http://center-bereg.ru/h1846.html
6. Buranov L. The importance of internet culture in the fight against cybercrime. 2018, https://ictnews.uz/uz/15/05/2018/cybercrime/
7. Kochkina L. Definition of the concept "cybercrime". Selected types of cybercrime // Siberian criminal procedural and criminalistic readings. 2017. № 3 (17). - P. 2.
8. WHAT IS A LEGAL VIOLATION Meliyeva Dilrabo Baxtiyarovna Mirzo Ulugbek district preschool and school education department methodologist-psychologist. ARTICLE.
9. CYBER SECURITY AGAINST CYBERCRIME Abduvaliyev Ulugbek Shavkat oglu Ishtixon district Internal Affairs Department Operational Search Service Criminal Investigation Division operational officer, lieutenant. ARTICLE.

INTERNATIONAL LEGAL DOCUMENTS

10. Budapest Convention on Cybercrime of November 23, 2001.
11. Agreement on cooperation in combating crimes in the field of information technology between the Commonwealth of Independent States (CIS) member states of September 28, 2018

NATIONAL NORMATIVE LEGAL DOCUMENTS

12. Criminal Code of the Republic of Uzbekistan. September 22, 1994.
13. Law "On Cybersecurity". April 15, 2022.
14. Code "On Administrative Liability". April 1, 1995.

INTERNET SOURCES USED:

15. https://lex.uz/
16. https://csec.uz/uz/
17. https://uz.wikipedia.org/wiki/Kiberjinoyat#Manbalar
18. https://www.amerikaovozi.com/a/a-36-2010-03-26-voa1-93371769/807021.html
19. http://center-bereg.ru/h1846.html
20. https://uz.wikipedia.org/
21. https://www.stationx.net/cybercrime-statistics/
22. https://www.udemere.uz/docs/cyber-security/cyber-security-money-making-threats
23. https://wordlyknowledge.uz/index.php/iqro/article/download/2816/4206/5280/
24. https://www.kaspersky.ru/resource-center/threats/what-is-cybercrime
25. https://kun.uz/news/2023/12/20/ozbekistonda-2023-yilda-55-mingta-kiberjinoyat-sodir-etildi
26. https://inha.uz/wp-content/uploads/2022/02/yoshlar-inha.pdf

27. https://yurkitob.uz/ru/books/download?id=38