THE TRANSNATIONAL NATURE OF CYBERCRIME AND INTERNATIONAL LEGAL FRAMEWORKS FOR ITS PREVENTION AND COMBATING

Ochilova Mashkhura Odil kizi
The University of World Economy and
Diplomacy Master student of the Faculty of International law
mashhuraochilova@gmail.com *+99890 487 48 45*
https://doi.org/10.5281/zenodo.20793102

Abstract. *This article analyzes the transnational nature of cybercrime, the main factors that give rise to it, and international legal mechanisms for combating it. The study is based on the fact that the development of the Internet and information and communication technologies has created new forms of crime, and cybercrime is characterized by the fact that it bypasses territorial borders, electronic evidence is located in different jurisdictions, and the complexity of identifying criminals. The article analyzes the United Nations approach to transnational crime, the Budapest Convention, and other international legal instruments. It also examines the role of states, non-state organizations, organized criminal groups, and individuals as subjects of cybercrime. The study concludes that in order to effectively combat cybercrime, it is necessary to strengthen international cooperation, improve mechanisms for working with electronic evidence, and harmonize national legislation with international standards.*

Keywords: *cybercrime, transnational crime, cyberspace, jurisdiction, electronic evidence, Budapest Convention, international cooperation.*

INTRODUCTION

The rapid development of information and communication technologies has a profound impact on all spheres of life in modern society. The Internet has fundamentally changed the way individuals, government agencies, business entities and other institutions of society organize and manage their activities. E-commerce, virtual banking services, distance learning, e-government and digital communication tools have created new opportunities for people and organizations. At the same time, this digital environment has also created a new tool and arena for criminals.

Cybercrime differs from traditional crime in a number of ways. First of all, it does not recognize territorial borders. A criminal can attack an information system in another country, use servers in a third country and harm citizens of another country while being located on the territory of one country. In addition, electronic evidence of a crime can be stored in a completely different jurisdiction from the country where the criminal or victim is located. This complicates the issues of investigation, prosecution, extradition and mutual legal assistance.

The United Nations defines transnational crimes as crimes that affect more than one country or have consequences in more than one country. The UN Convention against Transnational Organized Crime also defines a crime as transnational in nature if it is committed in more than one country, if it is committed in one country and has significant consequences in another country, or if it involves an organized criminal group operating in more than one country[1]. Cybercrime fully meets these criteria, as attacks carried out via the Internet transcend geographical boundaries. Today, combating cybercrime is not a matter that can be resolved solely within the framework of national legislation. In this area, issues such as international cooperation, the exchange of electronic evidence, the rapid exchange of information between

[1] United Nations Convention against Transnational Organized Crime, adopted 15 November 2000, entered into force 29 September 2003, 2225 UNTS 209 https://www.unodc.org/unodc/en/organized-crime/intro/UNTOC.html

competent authorities,

extradition, technical assistance, and the harmonization of legislation are of particular importance. From this point of view, the Budapest Convention is recognized as one of the most important international legal instruments in the fight against cybercrime[2]. This convention establishes the general framework for the criminalization of cybercrimes, procedural measures and international cooperation.

The purpose of this article is to analyze the transnational nature of cybercrime, the main factors that give rise to it, and the international legal mechanisms for combating it.

METHODS

The research was organized on the basis of the IMRAD approach. The article used the methods of formal-legal, comparative-legal, systematic analysis and logical analysis. Using the formal-legal method, international conventions, UN documents, the Budapest Convention, its additional protocols, and regulatory legal acts of some countries on the fight against cybercrime were analyzed. The comparative-legal method made it possible to compare international and regional approaches to the fight against cybercrime. In particular, the experience of the UN, the Council of Europe, the CIS, the SCO, and some countries was studied. Using the method of systematic analysis, the transnational nature of cybercrime, subjects, jurisdiction, and problems related to electronic evidence were assessed in an interconnected manner.

The source basis of the research was the UN Convention against Transnational Organized Crime, the Budapest Convention, resolutions of the UN General Assembly, UNODC materials, international scientific literature, and scientific works of foreign and local scientists on cybercrime.

RESULTS

Transnational nature of cybercrime. Research findings show that one of the main characteristics of cybercrime is its transnational nature. The architecture of the Internet allows information to be transmitted to different parts of the world in a short time. Therefore, the commission, consequences and evidence of cybercrime are often associated with more than one country. Article 3 of the UN Convention against Transnational Organized Crime sets out the main criteria for a transnational crime.

According to it, a crime is considered transnational if it is committed in more than one country, if it is committed in one country and prepared, planned or controlled in another country, if it is committed with the participation of an organized criminal group operating in more than one country, or if it has serious consequences in another country[3]. Almost all of these situations can be encountered in cybercrime.

For example, in cases of phishing attacks, malware distribution, credit card fraud, ransomware attacks and illegal access to databases, the perpetrator, the victim, the server, the financial transaction and the electronic evidence may be located in different countries. This complicates the application of the classic principle of territorial jurisdiction.

Jonathan Clough explains the complexity of cybercrime by the fact that it is committed using technological means, the evidence is in digital form and creates new procedural problems for law enforcement agencies[4].

[2] Council of Europe, Convention on Cybercrime (Budapest Convention) ETS No 185 (23 November 2001) https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

[3] United Nations Convention against Transnational Organized Crime, adopted 15 November 2000, entered into force 29 September 2003, 2225 UNTS 209 https://www.unodc.org/unodc/en/organized-crime/intro/UNTOC.html

[4] Jonathan Clough, Principles of Cybercrime (2nd edn, Cambridge University Press 2015).

Susan Brenner notes that cybercrime poses a serious challenge to traditional approaches to criminal jurisdiction[5]. These considerations indicate the need to view cybercrime not as a simple national crime, but as a complex phenomenon requiring international cooperation.

Key factors that create transnationality. There are several key factors that create the transnational nature of cybercrime.

Firstly, there is a global target base of Internet users. A criminal can attack a user or organization anywhere in the world, regardless of their geographical location. This makes cybercrime more widespread than traditional crimes.

Secondly, differences in national legislation create favorable conditions for criminals. An act that is considered a crime in one country may not be clearly criminalized in another. This complicates the processes of bringing criminals to justice, extradition, and obtaining evidence.

Ales Završnik emphasizes that differences in the definition and criminological characteristics of cybercrime are a significant problem in regulating this area[6].

Thirdly, there are complexities in working with electronic evidence. Electronic evidence consists of information that is rapidly changing, can be deleted, or encrypted. In addition, such evidence is often stored on servers in other countries. Therefore, rapid international legal assistance mechanisms are needed to obtain them. The Budapest Convention establishes procedural measures and international cooperation mechanisms taking this very problem into account[7].

Fourth, technical vulnerabilities are actively exploited by criminals. Deficiencies in information systems and software create opportunities for malware, DDoS attacks, phishing and ransomware attacks. Gordon and Ford indicate the role of technology in the commission of crimes as a separate criterion in identifying and classifying cybercrime[8].

Cybercrime actors. Analysis allows us to divide cybercrime actors into three main groups: states, organizations, and individuals.

States are one of the most powerful actors in cyberspace. They can use cyber tools for intelligence, strategic advantage, political pressure, or national security purposes. Richard Clarke and Robert Knake have identified cyberwarfare as a new threat to national security[9]. The technical, financial, and military capabilities of states make them one of the most influential actors in cyberspace.

The second group is made up of non-state organizations and organized criminal groups. They are primarily interested in financial gain. Ransomware, bank fraud, data theft, illicit trade, and money laundering through cryptoassets are common areas of activity for such groups.

David Wall describes cybercrime as the transformation of crime in the information age and argues that the Internet has significantly expanded the possibilities for committing crimes[10].

The third group is made up of individuals. They include novice hackers, professional hackers, political hackers, and cyberterrorist groups.

[5] Susan W Brenner, 'Cybercrime Jurisdiction' (2006) 46 Crime, Law and Social Change 189–206.

[6] Ales Završnik, 'Cybercrime Definitional Challenges and Criminological Particularities' (2008) 2 Masaryk University Journal of Law and Technology 1–10.

[7] Council of Europe, Convention on Cybercrime (Budapest Convention) ETS No 185 (23 November 2001) https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

[8] Samuel Gordon and Richard Ford, 'On the Definition and Classification of Cybercrime' (2006) 2 Journal in Computer Virology 13–20.

[9] Richard A Clarke and Robert K Knake, Cyber War: The Next Threat to National Security and What to Do About It (HarperCollins 2010).

[10] David S Wall, Cybercrime: The Transformation of Crime in the Information Age (Polity Press 2007).

Beginners often act for fun, show off, or to gain recognition in the hacker community.

Professional hackers, on the other hand, have sophisticated technical knowledge and skills and may engage in illegal access to information systems, obtaining data, and disrupting systems.

The main motive in political hacking is political views or ideological goals.

Cyberterrorist groups, on the other hand, seek to damage objects important to the state and society, and to create an atmosphere of fear and instability. Canetti et al. have studied the psychological impact of cyberattacks on people[11].

International legal mechanisms. One of the most important international legal instruments in the fight against cybercrime is the Budapest Convention. This convention was adopted in 2001 and regulates crimes against computer systems and information, computer-mediated crimes, certain content-related crimes, and copyright infringements. An important aspect of the Budapest Convention is that it provides not only substantive criminal law norms, but also procedural measures. In particular, it establishes mechanisms for the preservation of electronic evidence, search and seizure of computer data, collection of traffic data, and mutual legal assistance between states[12]. The Second Additional Protocol, adopted in 2022, aims to disclose electronic evidence and strengthen international cooperation[13]. A number of documents have also been adopted within the UN framework to combat cybercrime. In particular, UN General Assembly resolutions against the criminal use of information technologies call on states to strengthen national measures and develop international cooperation in this area[14]. In 2024, the UN General Assembly adopted a new convention against cybercrime, which aims to strengthen international cooperation against certain crimes committed through information and communication technologies[15].

A legal framework for combating cybercrime has also been developed within the CIS.

The CIS Inter-Parliamentary Assembly adopted a model law "On Combating Cybercrime" on October 28, 2010[16]. This model law is important as a model document serving to harmonize the national legislation of the CIS countries. Within the SCO, information security issues are considered in connection with the fight against terrorism, separatism and extremism.

The SCO agreements on cooperation in the field of international information security are aimed at ensuring cybersecurity at the regional level[17].

Significance for Uzbekistan. Digitalization processes are developing rapidly in Uzbekistan.

---

[11] D Canetti, M Gross, I Waismel-Manor, A Levanon and H Cohen, 'How Cyberattacks Terrorize: Cortisol and Personal Insecurity Jump in the Wake of Cyberattacks' (2017) 20(2) Cyberpsychology, Behavior, and Social Networking 72–77 https://doi.org/10.1089/cyber.2016.0338

[12] Council of Europe, Convention on Cybercrime (Budapest Convention) ETS No 185 (23 November 2001) https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

[13] Council of Europe, Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-operation and Disclosure of Electronic Evidence CETS No 224 (12 May 2022) https://www.coe.int/en/web/cybercrime/second-additional-protocol

[14] United Nations General Assembly, Combating the Criminal Misuse of Information Technologies UNGA Res 55/63 (2000) https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_55_63.pdf accessed 17 June 2026; UNGA Res 56/121 (2001) https://docs.un.org/en/A/RES/56/121

[15] United Nations General Assembly, United Nations Convention against Cybercrime UNGA Res 79/243 (24 December 2024) https://docs.un.org/en/A/RES/79/243

[16] Interparliamentary Assembly of Member Nations of the CIS, Model Law on Countering Cybercrime (Resolution No 35-12, 28 October 2010) https://iacis.ru/baza_dokumentov/modelnie_zakonodatelnie_akti

[17] Shanghai Cooperation Organisation, Agreement on Cooperation in the Field of International Information Security among the Member States of the Shanghai Cooperation Organisation (Yekaterinburg, 16 June 2009) http://eng.sectsco.org/documents

The "Digital Uzbekistan – 2030" strategy is an important document aimed at developing e-government, the digital economy and information technologies in the country[18]. However, with the expansion of digitalization, the need to combat cybercrime also increases. It is important for Uzbekistan to study international experience in combating cybercrime, improve mechanisms for working with electronic evidence, strengthen the system of information exchange between state bodies and develop international cooperation. The Presidential Decree No. PQ-17 of January 22, 2025 is noteworthy for its focus on improving the system of training personnel in the field of cybersecurity[19].

Although the legal framework for combating cybercrime is being formed in the legislation of Uzbekistan, the issues of transnational cybercrime, rapid storage of electronic evidence, international legal assistance and unified information exchange on cyber incidents require constant improvement.

ANALYSIS AND DISCUSSION

Analysis shows that the transnational nature of cybercrime is fundamentally changing not only the methods of committing crimes, but also the traditional legal mechanisms for combating them. While in traditional crimes the location of the crime, the location of the perpetrator and the victim are usually associated with one or two countries, in cybercrime these elements can be located in several countries at the same time. For example, a criminal may send malicious software from the territory of one country, use servers in another country for the attack, and the victim may be in a third country. It is possible that electronic evidence may be located in a data storage center in a fourth country. In this case, the question of which country should investigate the crime, which court should hear the case, and which country's legislation should be applied becomes complicated. It is precisely the problems associated with jurisdiction that are one of the weakest points in the fight against transnational cybercrime. Because while a certain act may be considered a crime in some countries, it may not be sufficiently criminalized in others. As a result, criminals have the opportunity to use legal loopholes to evade responsibility. Issues related to electronic evidence also require special attention. Electronic evidence can be changed, deleted or moved to other servers in a short time. Therefore, the slow operation of existing international legal assistance mechanisms can often lead to the loss of evidence. This reduces the efficiency of investigations and trials.

The results of the study show that the fight against cybercrime is not limited to strengthening criminal legislation. Procedural mechanisms, technical capabilities, international information exchange, training and interstate trust play an important role in this area.

The first main problem is the issue of jurisdiction. Cybercrime can begin in one state and have consequences in another. In such a situation, which state should conduct the investigation, which state should have judicial jurisdiction and which state should hold the perpetrator accountable becomes a complex issue. Brenner emphasizes that cybercrime raises the issue of jurisdiction to a more complex form than traditional crimes[20].

The second problem is related to electronic evidence. Electronic evidence can be easily deleted, modified or moved to other servers. Therefore, it is important to quickly preserve, authenticate and evaluate evidence as reliable evidence in court in cybercrime investigations.

[18] President of the Republic of Uzbekistan, Decree No. PF-6079 of 5 October 2020 on the Approval of the "Digital Uzbekistan – 2030" Strategy and Measures for Its Effective Implementation https://lex.uz/docs/5031048
[19] President of the Republic of Uzbekistan, Resolution No PQ–17 of 22 January 2025, On Measures to Improve the System of Training Personnel in the Field of Cybersecurity https://lex.uz/uz/docs/-7339006
[20] Susan W Brenner, 'Cybercrime Jurisdiction' (2006) 46 Crime, Law and Social Change 189–206.

The Budapest Convention is an important document that establishes a mechanism for the rapid preservation of electronic evidence[21].

The third problem is the differences between national laws. The lack of a single international definition of cybercrime and the fact that each country approaches it differently based on its own legal system increase the chances of criminals avoiding responsibility. Therefore, harmonizing international standards and national legislation is an urgent task.

The fourth problem is the slowness of international cooperation. Cybercrimes are committed quickly, and electronic evidence can disappear in a short time. Sending requests for legal assistance through traditional diplomatic channels takes a lot of time. Therefore, 24/7 contact points, central authorized bodies and rapid information exchange platforms are important.

The fifth problem is that technological development is moving faster than legislation.

Artificial intelligence, crypto-assets, darknet platforms, encrypted communication tools and automated malware are creating new opportunities for criminals. And legislation cannot always adapt quickly to such changes.

From this point of view, combating cybercrime requires a comprehensive approach at the national and international levels. This requires a combination of legal mechanisms, technical capabilities, institutional cooperation, and enhancing cybersecurity culture.

CONCLUSION

The results of the study showed that cybercrime is characterized by its transnational nature, which complicates the processes of its detection, investigation and prosecution. In particular, the location of the crime site, the perpetrator, the victim and electronic evidence in different countries creates jurisdictional problems. Therefore, it is important to create effective procedural mechanisms for working with electronic evidence and strengthen international cooperation. The Budapest Convention, the UN and other international documents constitute the main legal foundation in this area. For Uzbekistan, studying international experience, improving national legislation and increasing the capacity of specialists in the field of cybersecurity and working with electronic evidence are urgent tasks.

REFERENCES:

1. United Nations Convention against Transnational Organized Crime, adopted 15 November 2000, entered into force 29 September 2003, 2225
2. UNTS 209 https://www.unodc.org/unodc/en/organized-crime/intro/UNTOC.html.
3. Council of Europe, Convention on Cybercrime (Budapest Convention) ETS No 185 (23 November 2001) https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185.
4. Jonathan Clough, Principles of Cybercrime (2nd edn, Cambridge University Press 2015).
5. Susan W Brenner, 'Cybercrime Jurisdiction' (2006) 46 Crime, Law and Social Change 189–206.
6. Ales Završnik, 'Cybercrime Definitional Challenges and Criminological Particularities' (2008) 2 Masaryk University Journal of Law and Technology 1–10.
7. Samuel Gordon and Richard Ford, 'On the Definition and Classification of Cybercrime' (2006) 2 Journal in Computer Virology 13–20.

[21] Council of Europe, Convention on Cybercrime (Budapest Convention) ETS No 185 (23 November 2001) https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

8. Richard A Clarke and Robert K Knake, Cyber War: The Next Threat to National Security and What to Do About It (HarperCollins 2010).
9. David S Wall, Cybercrime: The Transformation of Crime in the Information Age (Polity Press 2007).
10. D Canetti, M Gross, I Waismel-Manor, A Levanon and H Cohen, 'How Cyberattacks Terrorize: Cortisol and Personal Insecurity Jump in the Wake of Cyberattacks' (2017) 20(2) Cyberpsychology, Behavior, and Social Networking 72–77 https://doi.org/10.1089/cyber.2016.0338.
11. Council of Europe, Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-operation and Disclosure of Electronic
12. Evidence CETS No 224 (12 May 2022) https://www.coe.int/en/web/cybercrime/second-additional-protocol.
13. United Nations General Assembly, Combating the Criminal Misuse of Information Technologies UNGA Res 55/63 (2000) https://www.itu.int/ITU-
14. D/cyb/cybersecurity/docs/UN_resolution_55_63.pdf accessed 17 June 2026; UNGA Res 56/121 (2001) https://docs.un.org/en/A/RES/56/121.
15. United Nations General Assembly, United Nations Convention against Cybercrime UNGA Res 79/243 (24 December 2024) https://docs.un.org/en/A/RES/79/243.
16. Interparliamentary Assembly of Member Nations of the CIS, Model Law on Countering Cybercrime (Resolution No 35-12, 28 October 2010) https://iacis.ru/baza_dokumentov/modelnie_zakonodatelnie_akti.
17. Shanghai Cooperation Organisation, Agreement on Cooperation in the Field of International Information Security among the Member States of the Shanghai Cooperation Organisation (Yekaterinburg, 16 June 2009) http://eng.sectsco.org/documents.
18. President of the Republic of Uzbekistan, Decree No. PF-6079 of 5 October 2020 on the Approval of the "Digital Uzbekistan – 2030" Strategy and Measures for Its Effective Implementation https://lex.uz/docs/5031048.
19. President of the Republic of Uzbekistan, Resolution No PQ–17 of 22 January 2025, On Measures to Improve the System of Training Personnel in the Field of Cybersecurity https://lex.uz/uz/docs/-7339006.