IMPROVING INTERNATIONAL LEGAL MECHANISMS FOR COMBATING TRANSNATIONAL CYBERCRIME

Umarova Nazokat Fakhriddinovna
Student of Tashkent state university of Law
Criminal justice faculty
unazokat05@gmail.com
https://orcid.org/0009-0003-7151-8595
https://doi.org/10.5281/zenodo.20483557

Abstract: This article analyzes international legal mechanisms for combating transnational cybercrime in the context of globalization and rapid technological development. Particular attention is devoted to international conventions, jurisdictional issues, cyberterrorism, digital evidence, and international cooperation among law enforcement agencies. The article also examines the legal framework of the Republic of Uzbekistan in the field of cybersecurity and proposes recommendations aimed at strengthening international cooperation and harmonizing domestic legislation with international standards.

Keywords: transnational cybercrime, cybersecurity, international law, Budapest Convention, cyberterrorism, digital evidence, international cooperation, jurisdiction, information security, cyber legislation.

Annotatsiya: Mazkur maqolada globallashuv va axborot texnologiyalarining jadal rivojlanishi sharoitida transmilliy kiberjinoyatchilikka qarshi kurashning xalqaro-huquqiy mexanizmlari tahlil qilinadi. Maqolada xalqaro konvensiyalar, yurisdiksiya muammolari, kiberterrorizm, raqamli dalillar hamda huquqni muhofaza qiluvchi organlar o‘rtasidagi xalqaro hamkorlik masalalariga alohida e’tibor qaratilgan. Shuningdek, O‘zbekiston Respublikasining kiberxavfsizlik sohasidagi qonunchiligi o‘rganilib, xalqaro hamkorlikni kuchaytirish hamda milliy qonunchilikni xalqaro standartlarga uyg‘unlashtirish yuzasidan takliflar ishlab chiqilgan.

Kalit so‘zlar: transmilliy kiberjinoyatchilik, kiberxavfsizlik, xalqaro huquq, Budapesht konvensiyasi, kiberterrorizm, raqamli dalillar, xalqaro hamkorlik, yurisdiksiya, axborot xavfsizligi, kiber qonunchilik.

Аннотация: В данной статье исследуются международно-правовые механизмы борьбы с транснациональной киберпреступностью в условиях глобализации и стремительного развития информационных технологий. Особое внимание уделяется международным конвенциям, вопросам юрисдикции, кибертерроризму, цифровым доказательствам и международному сотрудничеству правоохранительных органов. Кроме того, анализируется законодательство Республики Узбекистан в сфере кибербезопасности и предлагаются рекомендации по совершенствованию международного сотрудничества и гармонизации национального законодательства с международными стандартами.

Ключевые слова: транснациональная киберпреступность, кибербезопасность, международное право, Будапештская конвенция, кибертерроризм, цифровые доказательства, международное сотрудничество, юрисдикция, информационная безопасность, киберзаконодательство.

The rapid development of information technologies and digital globalization has significantly transformed modern society. Alongside technological progress, cyberspace has become increasingly vulnerable to criminal activities. Cybercrime today represents one of the most dangerous forms of transnational organized crime threatening economic stability, state sovereignty, public security, and fundamental human rights.[1]

Unlike traditional crimes, cybercrime possesses a borderless nature. Offenders may commit unlawful acts from one state while targeting victims located in another jurisdiction.[2] Such transnational characteristics create serious legal and practical challenges for criminal justice systems and require effective international legal cooperation. According to international analytical reports, global financial losses caused by cybercrime amount to trillions of dollars annually.[3] Cyberattacks targeting banking systems, healthcare institutions, governmental databases, and critical infrastructure continue to increase worldwide. Consequently, combating cybercrime has become one of the key priorities of international criminal policy and cybersecurity strategy. This article aims to analyze international legal mechanisms for combating transnational cybercrime, identify existing legal problems, and develop recommendations for improving international cooperation in this sphere.

Transnational cybercrime refers to criminal acts committed through information and communication technologies affecting multiple states simultaneously.[4]Cybercrime differs from traditional criminality due to anonymity, technical complexity, high latency, and the ability to rapidly cross national borders.

The main forms of cybercrime include: illegal access to computer systems, online financial fraud, identity theft, ransomware attacks, cyber espionage, dissemination of malicious software, cyberterrorism, attacks against critical infrastructure. The danger of cybercrime is intensified by the fact that digital technologies enable offenders to attack thousands of victims simultaneously with minimal financial resources.[5]

One of the most important international legal instruments regulating cybercrime is the Convention on Cybercrime adopted by the Council of Europe in 2001, commonly known as the Budapest Convention.[6] The Convention establishes harmonized legal standards concerning: criminalization of cyber offenses, procedural investigative powers, extradition procedures, mutual legal assistance, international cooperation mechanisms. The Budapest Convention obliges states to criminalize offenses such as illegal access, illegal interception, data interference, computer-related fraud, and child pornography offenses committed through information technologies.[7]

One of the Convention's most significant achievements is the establishment of the 24/7 international cooperation network facilitating rapid information exchange among law enforcement authorities.

[1] Susan W. Brenner, Cybercrime and the Law: Challenges, Issues, and Outcomes (Boston: Northeastern University Press, 2012), p. 45.
[2] Neil Boister, An Introduction to Transnational Criminal Law (Oxford: Oxford University Press, 2018), p. 93.
[3] Interpol, Global Cybercrime Strategy Report (Lyon: Interpol, 2023), p. 18.
[4] David S. Wall, Cybercrime: The Transformation of Crime in the Information Age (Cambridge: Polity Press, 2007), p. 21.
[5] Majid Yar and Kevin Steinmetz, Cybercrime and Society (London: Sage Publications, 2019), p. 102.
[6] Convention on Cybercrime (Budapest Convention), Council of Europe, Budapest, 23 November 2001.
[7] Jonathan Clough, Principles of Cybercrime (Cambridge: Cambridge University Press, 2015), p. 67.

The United Nations actively promotes international cybersecurity and cooperation against cybercrime. In particular, UN General Assembly Resolution No. 74/247 emphasized the necessity of developing an international convention aimed at countering the criminal use of information technologies[8]. The UN also highlights the importance of balancing cybersecurity measures with human rights protection, including privacy rights and freedom of expression.

Regional organizations also play an important role in combating cybercrime. Interpol coordinates international cybercrime investigations and facilitates intelligence sharing among member states[9]. Europol supports joint cybercrime operations within Europe and assists national authorities in investigating organized cybercriminal groups[10]. Furthermore, the European Union has adopted several cybersecurity strategies and legal acts aimed at strengthening digital resilience and harmonizing member states' legislation[11].

One of the major legal problems concerns jurisdiction. Cyber offenses often involve several states simultaneously because perpetrators, victims, servers, and financial systems may be located in different jurisdictions[12]. Traditional territorial principles of criminal jurisdiction are often ineffective in cyberspace. As a result, determining which state possesses investigative and judicial authority becomes extremely difficult.

Digital evidence constitutes one of the most important elements in cybercrime investigations. However, electronic evidence may easily be modified, deleted, or transferred across borders within seconds[13]. Moreover, states apply different standards concerning admissibility and authentication of electronic evidence, creating obstacles for international cooperation and judicial proceedings.

Cyberterrorism represents a serious threat to national and international security. Terrorist organizations increasingly use cyberspace for propaganda, recruitment, financing, and attacks against critical infrastructure[14].

Cyberattacks against energy systems, transportation networks, and governmental institutions may result in severe economic and social consequences.

Uzbekistan has implemented several reforms aimed at strengthening cybersecurity and combating cybercrime. National legislation criminalizes unauthorized access to computer information, dissemination of malicious software, cyber fraud, and illegal use of personal data[15]. The country actively participates in international cooperation concerning digital governance and cybersecurity policy. Nevertheless, several issues remain unresolved, including: insufficient digital forensic expertise, shortage of specialized investigators, limited international data exchange mechanisms, necessity for further harmonization with international legal standards. Further modernization of legislation and strengthening institutional capacity remain essential for ensuring effective cybersecurity in Uzbekistan.

[8] United Nations General Assembly Resolution No. 74/247 "Countering the Use of Information and Communications Technologies for Criminal Purposes," adopted 27 December 2019.
[9] Interpol, Global Cybercrime Strategy Report, p. 25.
[10] Europol, Internet Organised Crime Threat Assessment (The Hague, 2022), p. 34.
[11] European Union, The EU Cybersecurity Strategy for the Digital Decade (Brussels, 2020), p. 11.
[12] Marco Gercke, Understanding Cybercrime: Phenomena, Challenges and Legal Response (Geneva: ITU Publication, 2012), p. 56.
[13] Jonathan Clough, Principles of Cybercrime, p. 144.
[14] Michael Goodman, Future Crimes (New York: Anchor Books, 2016), p. 134.
[15] Criminal Code of the Republic of Uzbekistan, provisions concerning crimes in the sphere of information technologies.

The following measures may significantly improve international legal mechanisms against cybercrime: harmonization of national cybercrime legislation with international standards, expansion of international cooperation concerning digital investigations, development of unified standards for digital evidence collection and preservation, strengthening cybersecurity institutions and technical capacities, improvement of extradition and mutual legal assistance procedures, adoption of new international legal instruments addressing emerging cyber threats and artificial intelligence-related crimes.

Conclusion: Transnational cybercrime represents one of the most serious threats of the digital age. Due to its borderless nature, no state can independently combat cybercrime effectively. International legal cooperation, harmonization of legislation, and effective exchange of information remain crucial elements in ensuring global cybersecurity. The Budapest Convention, United Nations initiatives, and regional cooperation mechanisms form the foundation of the international legal framework against cybercrime. Nevertheless, rapid technological development continuously creates new legal challenges requiring modernization of both international and domestic legislation. Uzbekistan should continue improving its cybersecurity policy, strengthening legal regulation, and expanding international cooperation to ensure effective protection against cyber threats and transnational cybercrime.

References:

Boister, Neil. An Introduction to Transnational Criminal Law. Oxford: Oxford University Press, 2018;

Brenner, Susan W. Cybercrime and the Law: Challenges, Issues, and Outcomes. Boston: Northeastern University Press, 2012;

Clough, Jonathan. Principles of Cybercrime. Cambridge: Cambridge University Press, 2015;

Convention on Cybercrime (Budapest Convention). Council of Europe, 2001;

Europol. Internet Organised Crime Threat Assessment. The Hague, 2022;

European Union. The EU Cybersecurity Strategy for the Digital Decade. Brussels, 2020;

Gercke, Marco. Understanding Cybercrime: Phenomena, Challenges and Legal Response. Geneva: ITU Publication, 2012;

Goodman, Michael. Future Crimes. New York: Anchor Books, 2016;

Interpol. Global Cybercrime Strategy Report. Lyon, 2023;

United Nations General Assembly Resolution No. 74/247 “Countering the Use of Information and Communications Technologies for Criminal Purposes,” 2019;

Wall, David S. Cybercrime: The Transformation of Crime in the Information Age. Cambridge: Polity Press, 2007;

Yar, Majid, and Kevin Steinmetz. Cybercrime and Society. London: Sage Publications, 2019.