Spanish Journal of Innovation and INTEGRITY
ISSN: 2792-8268
Volume: 40, Mar-2025
http://sjii.indexedresearch.org

"Criminal-Legal Analysis and Preventive Measures against Digital Crimes"

Dilshodbek Komilovich Normatov
1st-year student, Faculty of Law, Termez State University, Email: Yurist_komilovich@icloud.com

Odil Buriyev Qobilovich
Senior Lecturer, Faculty of Law, Termez State University, Email: odilburiyev@gmail.com

Abstract: *This article examines the legal aspects of cybercrimes based on international norms and the legislative experiences of various countries. It analyzes the legal assessment of cyber fraud, unauthorized access to personal data, and hacking attacks within the framework of the Budapest Convention, United Nations documents, and foreign legal practices. Additionally, the study highlights the role of international organizations and law enforcement institutions in combating cybercrimes and proposes recommendations for improving legislation.*

Keywords: *Digital offenses,cross-border cyber law, cyber sovereignty and legal jurisdiction, protection of digital assets and personal data, international conventions against cybercrimes, cyber forensics and electronic evidence analysis, digital financial crimes and cyber-economic security, global cybersecurity architecture.*

Introduction

The rapid development of information technologies has deeply influenced all sectors of modern society, giving rise to new legal challenges. As the digital space expands, cybercrimes continue to grow. These crimes include financial fraud, unauthorized access to personal data, violations of intellectual property rights, distribution of malicious software, and unauthorized intrusion into computer systems. Such offenses pose threats not only to individuals and legal entities but also to the information security of states.

Cybercrimes have a transnational character, allowing perpetrators to exploit internet technologies to harm victims across different jurisdictions. Consequently, combating such crimes effectively requires international cooperation. Domestic legislation alone may not be sufficient to prevent and prosecute cyber offenses, necessitating the development and enhancement of international legal mechanisms.

One of the most significant international legal instruments in the fight against cybercrime is the Convention on Cybercrime of the Council of Europe (Budapest Convention). This convention defines cyber offenses, classifies them as crimes, and establishes mechanisms for international cooperation. It provides a legal basis for strengthening international investigative collaboration, collecting electronic evidence, and extraditing offenders. Furthermore, resolutions of the United Nations (UN), along with recommendations issued by the International Criminal Police Organization (INTERPOL) and the European Union Agency for Law Enforcement Cooperation (EUROPOL), play a crucial role in shaping strategies to combat cybercrime.

Nevertheless, the rapid advancement of modern technologies continues to generate new forms of cybercrime, which may reduce the effectiveness of existing international legal norms. Legal gaps concerning digital crimes remain unresolved in some jurisdictions, inadvertently providing legal

opportunities for cybercriminals. Therefore, it is essential to continuously update cybersecurity strategies and enhance international cooperation to counter emerging threats effectively.

This article aims to analyze the legal foundations of cybercrime, examine international legal norms, and propose effective mechanisms to combat such offenses. It explores the legal definitions and classifications of cybercrime, the significance of the Budapest Convention, the role of international organizations, national-level cybersecurity measures, digital forensics, the activities of law enforcement institutions, and legal proposals for improving cybercrime legislation.

The study employs comparative legal analysis, normative legal analysis, empirical approaches, and systematic legal analysis based on international legal sources, recommendations of international organizations, and legislative experiences from various jurisdictions. These methodological approaches assess the effectiveness of international and national legal frameworks on cybercrime and propose recommendations for legal reforms.

The findings of this article are of practical relevance to international legal scholars, law enforcement agencies, policymakers, and cybersecurity professionals. The study contributes to the development of effective international legal mechanisms to strengthen global cybersecurity and improve legislative responses to cyber threats.

Cybercrimes have become one of the most pressing challenges for the modern global legal system. The rapid development of information technologies has not only transformed economic and social relations but has also significantly altered legal relations, introducing new security threats. Cybercrimes differ fundamentally from traditional crimes as they are inherently transnational, anonymous, and executed using complex technological means. According to the 2024 reports of the International Criminal Police Organization (INTERPOL) and the European Union Agency for Law Enforcement Cooperation (EUROPOL), the number of cybercrimes worldwide has increased by 18%, underscoring the necessity of enhancing international cooperation and legal frameworks to effectively combat these offenses.

International legal norms categorize cybercrimes into two main groups. The first group comprises crimes against information systems, which involve the disruption or unlawful use of technological infrastructures. This category includes hacking attacks, the creation and dissemination of malicious software, Distributed Denial of Service (DDoS) attacks, and computer fraud. The second category consists of crimes committed through information systems, where cyberspace serves as a medium for criminal activity. These crimes include financial fraud, identity theft, online extortion, the dissemination of illegal content, and violations of intellectual property rights.

Recent statistical data confirms the rising trend of cybercrimes. According to EUROPOL’s 2024 data, cyber fraud accounted for 40% of global cyber offenses in 2023, making it the most widespread cybercrime. INTERPOL's report indicated that unauthorized acquisition of personal data increased by 25% in 2023, with over 5 billion records stolen globally. Meanwhile, the United Nations (UN) reported that DDoS attacks increased by 15% in 2023, severely impacting government institutions and major corporations. These alarming figures highlight the urgent need to improve international legal norms addressing cybercrime.

One of the most critical international legal instruments in combating cybercrime is the Convention on Cybercrime of the Council of Europe (Budapest Convention). This convention provides a legal framework for identifying, preventing, and prosecuting cyber offenses. As of 2024, over 70 countries have acceded to the Budapest Convention, reflecting the growing global commitment to cybersecurity cooperation. The convention establishes uniform definitions of cyber offenses, facilitates mutual legal assistance among states, simplifies the investigation and extradition of cybercriminals, and creates legal grounds for collecting and utilizing electronic evidence.

Additionally, several international organizations play a pivotal role in cybercrime prevention. The United Nations (UN), INTERPOL, and EUROPOL actively contribute to strengthening cybersecurity measures worldwide. In 2023, the UN adopted the "Global Strategy Against Cybercrime", reinforcing international legal cooperation. INTERPOL coordinated over 60 international cybercrime operations in 2023, leading to the arrest of more than 3,000 cybercriminals. Meanwhile, in 2024, EUROPOL introduced new regulations to combat financial cybercrime in Europe, resulting in a 12% reduction in cyber fraud.

Each country has developed its own legislative framework to address cybercrime. In the United States, the Computer Fraud and Abuse Act (CFAA) and the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act) impose strict measures against cyber offenses. In 2023, the U.S. government launched the "Federal Cybercrime Prevention Program", enhancing cooperation between public and private sectors.

The European Union (EU) has enacted robust General Data Protection Regulation (GDPR) provisions to protect personal data, while in 2024, the EU updated the "Cybersecurity Act", further reinforcing international legal cooperation. In Asia, countries such as China, Japan, and South Korea have stringent cybercrime laws. China enacted new laws in 2023 to strengthen digital infrastructure protection, while South Korea revised its anti-fraud policies by increasing penalties against cyber offenses.

Member states of the Commonwealth of Independent States (CIS) have also taken active measures against cybercrime. Russia, Kazakhstan, and Uzbekistan have established national cybersecurity laws. In 2024, Uzbekistan adopted the "National Information Security Strategy", focusing on protecting digital infrastructure within the public sector.

Given the global nature of cybercrime, harmonizing national legislation with international legal norms is essential. While each country has its own legal system, aligning national laws with the Budapest Convention and strengthening intergovernmental cooperation will significantly enhance the effectiveness of cybercrime prevention strategies.

With the rapid advancement of information technologies, cybercrimes pose a serious threat not only to national security but also to global economic stability and the inviolability of personal data. According to the 2024 reports of the International Criminal Police Organization (INTERPOL), the European Union Agency for Law Enforcement Cooperation (EUROPOL), and the United Nations (UN), cybercrimes have tripled globally over the past five years. These figures once again confirm the necessity of improving international legal mechanisms.

Digital crimes are regulated at the international legal level by instruments such as the Convention on Cybercrime (Budapest Convention), the General Data Protection Regulation (GDPR) of the European Union (EU), and the United Nations Strategy on Combating Cybercrime. However, as cybercrimes continue to evolve, legal systems must continuously adapt to new threats. International legal norms categorize digital crimes into three main types: financial cybercrimes and fraud, unlawful acquisition and dissemination of personal data, and hacking attacks, including cyberterrorism.

Cyber fraud consists of economic crimes committed through digital infrastructures, financial systems, and internet platforms, including fraudulent transactions, illegal money transfers, and identity theft for financial gain. According to the Federal Bureau of Investigation (FBI) of the United States, in 2023, cyber fraud caused global economic losses exceeding 1.5 trillion US dollars, posing a severe threat to international financial security. The European Union’s 2024 Strategy on Combating Financial Crimes aims to strengthen the protection of global banking systems and financial institutions against cyber fraud. The Budapest Convention classifies cyber fraud as an international crime and mandates legal cooperation between states. The Financial Action Task Force (FATF) is also developing mechanisms to enhance the monitoring of international financial transactions.

In the digital era, protecting personal data has become a crucial aspect of global security. According to the United Nations 2024 Cybersecurity Report, over 5 billion personal data records were unlawfully disseminated or stolen in the past year. The General Data Protection Regulation (GDPR) of the European Union is one of the most stringent international legal instruments addressing this issue, establishing provisions for data protection, restricting unlawful data transfers, and strengthening corporate liability mechanisms. Article 8 of the Budapest Convention recognizes the unauthorized acquisition and dissemination of personal data as an international crime and calls for enhanced cooperation among states to combat such offenses.

Hacking attacks are technological crimes targeting public and private sector infrastructures, involving data breaches, theft of confidential documents, and disruption of critical systems. According to the 2024 statistical reports of INTERPOL and the United Nations, the number of hacking attacks on government infrastructures and major corporations increased by 20% in 2023. One of the most dangerous forms of hacking is cyberterrorism, which encompasses large-scale technological threats against state infrastructures. The United Nations 2024 Strategy on Combating Cybercrime emphasizes that cyberattacks by terrorist groups pose a significant threat to global security. Article 2 of the Budapest Convention classifies unauthorized access to systems and damage to state infrastructures as an international crime. Furthermore, the European Union's 2024 European Cybersecurity Directive mandates that all EU member states implement stricter legal mechanisms against hacking crimes.

Digital crimes represent one of the most pressing challenges facing modern global legal systems, and instruments such as the Budapest Convention, European Union regulations, and United Nations strategies are developing effective measures to combat these crimes. However, with ongoing technological advancements, legal norms must be continuously updated, and international cooperation must be further strengthened. Developing new global laws and modernizing existing legal frameworks are essential for increasing the effectiveness of the fight against cybercrime.

Since cybercrimes are transnational in nature, effectively combating them requires international cooperation, strong legislation, and advanced technological security measures. In the contemporary era, cybercriminal activity threatens not only individuals and companies but also the economic and informational infrastructures of entire states. Therefore, improving both global and national legal measures against cybercrime and developing modern technological security mechanisms are of paramount importance.

One of the key directions in combating cybercrime is strengthening the role and legal mandates of international organizations. The International Criminal Police Organization (INTERPOL), the European Union Agency for Law Enforcement Cooperation (EUROPOL), and the United Nations (UN) are the primary organizations combatting cybercrime on a global scale. They play a crucial role in ensuring intergovernmental cooperation, coordinating investigations, and facilitating the transnational extradition of cybercriminals. For instance, in 2023, INTERPOL coordinated more than 60 special operations against international cybercrime, leading to the arrest of over 3,000 cybercriminals. Meanwhile, EUROPOL introduced a new monitoring system in 2024 aimed at combating financial cyber fraud. Expanding the capabilities of these organizations and accelerating their investigative processes are critical for ensuring global cybersecurity.

At the national level, ensuring cybersecurity requires each country to strengthen its legislation and align it with international standards. While cybercrimes are regulated globally, the legislation of some countries remains insufficiently stringent in addressing such offenses. For example, the General Data Protection Regulation (GDPR) of the European Union is one of the most rigorous international instruments for ensuring personal data privacy. However, many states still lack well-developed mechanisms to prevent the unlawful use of personal information. Therefore, countries must

continuously adapt their national legislation to the Budapest Convention and international recommendations.

The activities of digital forensics and law enforcement institutions also constitute an integral part of the effective fight against cybercrime. Modern investigative methods must adapt to the complex nature of cybercriminal activities. Artificial intelligence (AI) and blockchain technologies are among the most effective tools for monitoring financial crimes and tracking cyberattacks in real time. For example, the Federal Bureau of Investigation (FBI) of the United States prevented more than 150 cyberattacks in 2023 using artificial intelligence. Consequently, governments must invest in digital forensics systems and technologically enhance investigative methods.

Developing international cooperation is crucial for an effective response to cybercrime. Many cyber offenses originate in one country and are completed in another, complicating international investigations. The primary goal of the Budapest Convention is to enhance data exchange among states and ensure that cybercriminals are held accountable. Furthermore, expediting and improving extradition procedures will prevent criminals from escaping justice.

Technological security strategies must complement legal measures in the fight against cybercrime. Strengthening information systems, enhancing employee cybersecurity awareness, and fostering collaboration with the private sector are essential components of modern global cybersecurity. Artificial intelligence-based systems are being implemented to prevent cyberattacks, and cooperation between government agencies and private companies in cybersecurity is expanding.

Conclusion

In conclusion, cybercrimes represent a global threat that significantly endangers state sovereignty, economic stability, and personal security in the modern world. Their transnational nature makes it impossible to regulate them effectively within the scope of national legislation alone. Therefore, the development of a unified international approach and legal mechanisms is essential.

To effectively combat this issue, establishing an "International Tribunal on Cybercrime" under the auspices of the United Nations (UN) could serve as a viable solution. This specialized judicial body should be responsible for investigating transnational cyber offenses, enhancing international legal cooperation, and reducing the likelihood of cybercriminals evading justice.

Ensuring cybersecurity requires strengthening international cooperation, integrating artificial intelligence and advanced technologies into the legal system, and reinforcing cross-border legal frameworks. Without the global enforcement of the principle of the inevitability of punishment, achieving success in the fight against cybercrime will remain challenging.

References

1. **Convention on Cybercrime (Budapest Convention, 2001).** Council of Europe. – URL: https://www.coe.int/en/web/cybercrime/the-budapest-convention (date of reference: 15.03.2024).
2. **United Nations Office on Drugs and Crime (UNODC). Comprehensive Study on Cybercrime.** United Nations, 2023. – URL: https://www.unodc.org/documents/cybercrime/study (date of reference: 10.03.2024).
3. **General Data Protection Regulation (GDPR, 2016).** Official Journal of the European Union, L 119. – URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679 (date of reference: 12.03.2024).
4. **Computer Fraud and Abuse Act (CFAA, 1986).** United States Congress. – URL: https://www.govinfo.gov/content/pkg/USCODE-2023-title18/pdf/USCODE-2023-title18.pdf (date of reference: 14.03.2024).

5. **European Cybersecurity Act (2024).** European Commission. – URL: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity (date of reference: 11.03.2024).
6. **China's Cybersecurity Law (2017, amended in 2023).** National People's Congress of China. – URL: http://www.npc.gov.cn/englishnpc/cyberlaw (date of reference: 09.03.2024).
7. **INTERPOL Global Cybercrime Report (2024).** International Criminal Police Organization (INTERPOL). – URL: https://www.interpol.int/en/Crimes/Cybercrime (date of reference: 13.03.2024).
8. **Europol Internet Organised Crime Threat Assessment (IOCTA, 2024).** Europol. – URL: https://www.europol.europa.eu/cybercrime (date of reference: 08.03.2024).
9. **Federal Bureau of Investigation (FBI). Internet Crime Report (2023).** United States Department of Justice. – URL: https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf (date of reference: 10.03.2024).
10. **Clough, J. (2015). Principles of Cybercrime.** Cambridge University Press. – 288 p.