American Journal of Open University Education
ISSN 2997-3899
Vol. 2, No. 5, May 2025,
Available online at: https://scientificbulletin.com/index.php/AJOUP

Specific Aspects of the Activities of International and Regional Organizations in Preventing Cybercrime

Samadova Marjona Bohodir kizi
Tashkent State University of Law Master's student in the field of media law

Article information:
Manuscript received: 28 Mar 2025; **Accepted:** 27 Apr 2025; **Published:** 31 May 2025

Annotation: This article is devoted to the role and specific activities of international and regional organizations in preventing cybercrimes. The article highlights the importance of international cooperation, taking into account the global nature of cybersecurity threats. Using the example of various organizations (UN, Interpol, OSCE, Shanghai Cooperation Organization, etc.), their strategies, mechanisms and ways of exchanging experience are analyzed. Their impact on national cybersecurity systems and prospects for future cooperation are also considered. Abstract This article is devoted to the role and specific activities of international and regional organizations in preventing cybercrimes. The article highlights the importance of international cooperation, taking into account the global nature of cybersecurity threats. Furthermore, it examines their impact on national cybersecurity frameworks and prospects for future collaboration.

With the expansion of the cyber world and the rapid development of digital technologies, cybercrimes have become a serious threat on a global scale. Cybercrimes do not recognize national borders, which shows that unified national efforts are insufficient to combat them. Therefore, international and regional organizations play a crucial role in preventing and combating cybercrime. Their activities provide coordination, expertise, and exchange, unification of the legal framework and provision of technical assistance.

Cybercrimes, in particular, data theft, financial fraud, cyberterrorism and attacks on state information systems, threaten not only the security of a single state, but also the economy and stability of the entire world. Effectively combating such global threats requires harmonizing national security measures with international efforts. This is where international organizations play a central role. They create an open forum for dialogue between states, develop common strategies and set global standards for cybersecurity.

United Nations (UN): The UN considers cybersecurity in the context of international peace and security. Its Governmental Expert Groups (GGE) on Cybersecurity develop recommendations on setting norms of behavior of states in cyberspace, non-violent conflict resolution and confidence-building measures. The UN Office on Drugs and Crime (UNODC) also implements technical assistance and capacity-building programs in the fight against cybercrime. They mainly focus on the criminal and legal aspects of cybercrime. Interpol (International Criminal Police Organization): Interpol provides cooperation between police forces in the investigation and prevention of cybercrime. Its Global Cybercrime Center (IGCI) conducts training aimed at exchanging information on cybersecurity threats, providing technical assistance in solving cybercrimes, and improving the cyber capacity of law enforcement agencies. The

use of Interpol databases and networks allows for the cross-border tracking and arrest of cybercriminals. The UN's work in the field of cybersecurity is carried out in several directions. One of them is the formation of an international legal framework. Special resolutions on "International Security in the Information and Telecommunications Sector" are adopted within the framework of the UN General Assembly. Since 1998, new documents have been developed annually on the basis of an initiative put forward by the Russian Federation. These resolutions cover issues such as cybersecurity principles, confidence-building measures, interstate information exchange, and harmonization of national policies. The UN has specialized structures to combat cybercrime. For example, UNODC (United Nations Office on Drugs and Crime) is one of the most active agencies in this regard, providing technical assistance to countries, helping to improve legislation, and organizing training for investigators. Through the "Global Program to Combat Cybercrime" developed by UNODC, developing countries have the opportunity to strengthen their capacity to combat cybercrime. Also, the UN Secretary-General's Governmental Group of Experts (GGE) and Open-Ended Working Group (OEWG) play an important role in promoting inter-state dialogue, building confidence, and applying international legal principles in cybersecurity. The recommendations developed by these groups are used as a roadmap by UN Member States. Within the UN, the Digital Cooperation Roadmap (developed in 2020) is also an important initiative designed to improve digital security and Internet governance, ensure digital equality, and protect human rights. Through this roadmap, countries are working together to reduce the digital divide, increase the safety of Internet use, and ensure the digital rights of citizens. At the same time, the UN's role in combating cybercrime is not limited to political initiatives. Practical assistance is also provided within the organization through information exchange, dissemination of best practices, and support for national institutions. This serves to improve international mechanisms for preventing, detecting and investigating cybercrime. At a time when cybercrime is becoming increasingly important as a global problem, international cooperation and coordinated action are of great importance.

In this regard, INTERPOL - the International Criminal Police Organization - is one of the most important and active international structures. Its main task is to exchange information, take rapid measures and establish technical cooperation in combating transnational crimes. INTERPOL operates in several strategic areas in combating cybercrime. Established in 2015, the INTERPOL Cybercrime Directorate - that is, the Cybercrime Department - is one of the leading centers for combating, preventing and investigating cybercrime on a global scale. The headquarters of this department are located in the INTERPOL Global Complex for Innovation (IGCI) in Singapore, where advanced technologies, analytical tools and experts operate. One of INTERPOL's main areas of activity is to establish a real-time exchange of information on cybercrime among its 195 member states. Through the organization's global information system called i-24/7, countries quickly share information about crime with each other. This system helps to quickly identify and eliminate cases of, in particular, phishing, hacking, malware distribution, fraud and financial crimes committed via the Internet. Another important aspect is that INTERPOL has established cooperation with the private sector and other international organizations. For example, INTERPOL is working with Microsoft, Trend Micro, Kaspersky Lab, Cisco and other technology giants to jointly combat new threats and risks. This cooperation creates the opportunity to strengthen security in the cyber environment, use advanced technological tools and prevent crimes. INTERPOL's Cyber Fusion Centre serves as a centralized analysis and coordination center for combating global cybercrime. This center analyzes information received from various sources, communicates it to its members and encourages them to take prompt action. In conclusion, INTERPOL is today one of the important institutional foundations of the global fight against cybercrime. Its activities through information exchange, technical assistance, training and international cooperation are of great importance in ensuring global security.

Organization for Security and Cooperation in Europe (OSCE): The OSCE sees cybersecurity as a means of strengthening regional stability and confidence. Its activities are aimed at developing confidence-building measures, creating mechanisms for exchanging information on cyberattacks, and assisting member states in developing cybersecurity strategies. The OSCE promotes dialogue between states by

organizing seminars and conferences on cybersecurity. Cybercrime today is not only a financial and technical threat, but also a serious problem for international security and political stability. Therefore, the work of international organizations, in particular the Organization for Security and Cooperation in Europe (OSCE), is becoming increasingly relevant. The OSCE is the largest regional security organization, uniting 57 states, and it applies a comprehensive security approach in its activities. The OSCE implements its main areas of activity on cybersecurity based on the concept of "Confidence Building Measures" (CBMs). The CBM package, adopted by the OSCE Permanent Council in 2013, is aimed at strengthening trust between the member states of the organization, increasing openness in the use of information and communication technologies and reducing risks in the field of cybersecurity. Through dialogue platforms, seminars and technical expert meetings organized by the OSCE, member states exchange experience in combating cybercrime. The organization regularly advises on the development of national cybersecurity strategies, helps strengthen the regulatory framework and provides technical assistance in implementing security sector reforms. The organization also promotes an approach that takes into account the gender aspects of cybercrime. The organization has developed separate programs to ensure women's digital safety, create equal access to digital technologies, and combat gender-based cyberviolence. Through this approach, the OSCE approaches cybersecurity in a way that integrates human rights and gender equality.

The OSCE offices in Central Asia, including Uzbekistan, are also actively involved in this area. The organization, in cooperation with Uzbekistan, organizes cybersecurity training courses, legislative consultations, and public awareness campaigns. This helps to strengthen national capacities and create systems that meet international standards. Regional organizations can provide more targeted and rapid solutions due to geographical proximity and common interests. While cybercrime is a global problem, it also poses various threats and risks at the regional level. Therefore, along with international initiatives, regional organizations are increasingly actively involved in cybersecurity. These organizations play an important role in combating cybercrime within their regions through information exchange, capacity building, policy coordination, and technical assistance. Within the CIS (Commonwealth of Independent States), information security issues are discussed at high-level meetings.

Based on the "Concept of Ensuring Information Security", adopted in 2001, the CIS countries cooperate in combating the illegal use of information technologies, harmonizing national legislation and exchanging experience. The Shanghai Cooperation Organization (SCO) also pays special attention to cybersecurity issues. The "Cybersecurity Cooperation Plan" has been implemented within the organization since 2009. Documents have been signed between the SCO countries to prevent the use of information technologies for the purposes of terrorism, extremism and separatism. The SCO Regional Anti-Terrorism Structure (RATS) has also been established between the countries, which has created information bases to combat cybercrime. Another active regional organization is ASEAN (Association of Southeast Asian Nations). Within ASEAN, the "ASEAN Cybersecurity Cooperation Strategy" has been developed, which aims to promote technical cooperation, policy consultation and the development of standards on cybersecurity among member states. The ASEAN-Japan Cybersecurity Capacity Building Centre, established by ASEAN, is playing an important role in improving the skills of specialists in the region. The African Union is also developing its own policy on digital security. The "Malabo Convention" (African Union Convention on Cyber Security and Personal Data Protection), adopted in 2014, created the first legal framework for African countries in the digital sphere. This convention aims to create a single regional framework for information security, personal data protection and combating cybercrime. Regional organizations complement and strengthen international efforts to combat cybercrime in their regions through a unified approach, information exchange, the development of strategic documents and the development of national capacities. In conclusion, the role of international and regional organizations in preventing cybercrime is invaluable. They provide a comprehensive approach to global threats, develop effective cooperation between states, and set global and regional standards for strengthening cybersecurity. The specific features of the activities of these organizations make them key pillars in building a cyber-secure future. For countries like Uzbekistan,

cooperation with these organizations is very important in improving the national cybersecurity system.

List of References:

1. United Nations. General Assembly Resolution A/RES/68/243: Ensuring security in the field of information and telecommunications technologies and their use. December 27, 2013.
2. Interpol. Global Cybercrime Programme. Official website. URL: https://www.interpol.int/Crimes/Cybercrime/Global-Cybercrime-Programme(Accessed: 27.05.2025)
3. Organization for Security and Cooperation in Europe (OSCE). Cybersecurity Confidence-Building Measures. Official website. URL: https://www.osce.org/chairmanship/cyber-confidence-building-measures (Accessed: 27.05.2025)
4. Shanghai Cooperation Organization. Agreement on Cooperation in the Field of Ensuring Information Security. June 16, 2009.
5. Commonwealth of Independent States. Agreement on Cooperation in the Field of Informatization, Information Security and Information Technologies. (The relevant CIS document must be identified, usually agreements exist).
6. ENISA (European Agency for Cybersecurity). Official website. URL: https://www.enisa.europa.eu/ (Access date: 27.05.2025)
7. European Parliament and Council. Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation - GDPR). April 27, 2016.
8. CIS Information Security Concept (2001).
9. Shanghai Cooperation Organization (SCO) – Regional Anti-Terrorist Structure. http://eng.sectsco.org/
10. African Union – Malabo Convention. https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection