JOURNAL OF MULTIDISCIPLINARY SCIENCES AND INNOVATIONS
GERMAN INTERNATIONAL JOURNALS COMPANY
ISSN: 2751-4390
IMPACT FACTOR (RESEARCH BIB) : 9,08. Academic research index

STATE AND PROBLEMS OF INTERNATIONAL COOPERATION IN THE FIGHT AGAINST TRANSNATIONAL CRIMES IN THE FIELD OF INFORMATION TECHNOLOGIES

Jonuzokova Yulduz Izzatulla kizi

Doctoral student of the University of World Economy and Diplomacy

Abstract: Transnational cybercrime is one of the greatest threats to international security today. With the rapid development of digital technologies and Internet resources, criminals are finding new ways to use information technology for illegal activities, including data theft, system hacking, espionage, malware distribution, and financial fraud.

Keywords: cybercrime, information technology, hacking, espionage, malware distribution, and financial fraud, digital technologies.

Introduction. Since crimes committed in the digital space are not limited by geographical borders, their transnational nature requires joint efforts of states and international organizations to effectively combat them. However, the current state of international cooperation still faces a number of significant challenges, such as differences in legislation, jurisdictional barriers, political and cultural confrontations.

In recent years, due to the rapid development of digital technologies, the increase in the number of Internet users and the increase in the number of devices connected to the network, crimes in the field have grown significantly. Statistical data from various sources, such as Europol, Interpol, the US Federal Bureau of Investigation, and analytical reports from cybersecurity companies, confirm this trend. In particular, financial losses from crimes in the digital space have increased significantly in 2023-2024. Global losses are forecast to reach $9.5 trillion in 2024. By 2025, losses are expected to reach $10.5 trillion. [1]

Such losses are associated with ransomware attacks (malicious software that locks or encrypts a device and extorts money from the user), data leaks, DDoS attacks (Denial-of-service) - denial-of-service attacks. Sending a large number of requests to a web resource, causing it to stop working) and theft of personal information.

Methodology.

These losses are related to ransomware attacks (malicious software that locks or encrypts a device and extorts money from the user), data leaks, DDoS attacks (Denial-of-service) - denial of service. Sending a large number of requests to a web resource, causing it to stop working), and theft of personal information.

In 2023, 72.7 percent of organizations worldwide reported being victims of ransomware attacks. Although the overall volume of attacks decreased slightly compared to 2022, the complexity and destructiveness of such attacks increased. In 2023, more than 1,800 ransomware Trojans were identified that were designed to attack mobile devices. The attacks were mainly carried out on healthcare institutions, infrastructure companies, and educational institutions.

Data breaches remain one of the biggest threats to organizations worldwide in 2023-2024. Data

breaches are caused by hacking, insider attacks, or employee errors. The average cost to organizations is $4.35 million per incident.

While the number of DDoS attacks continues to grow in 2024, they are also becoming more sophisticated and multifaceted. Criminals are combining different attack vectors, making them more difficult to detect and neutralize. DDoS attacks are increasingly targeting key industries such as energy, telecommunications, healthcare, and financial systems.

Today, there are various initiatives and organizations that coordinate the actions of countries to combat transnational crime in the field of information technology on an international scale. One of the most important platforms for mutual cooperation is Interpol, which is engaged in the detection and investigation of crimes in different countries. Interpol supports global operations to combat cybercrime, in particular, projects such as DarkNet monitoring and tracking cyberattacks aimed at critical infrastructure.

Results and Discussion.

Interpol is coordinating and coordinating global operations to combat cybercrime, uniting law enforcement agencies from around the world. One such operation, HAECHI-III, was conducted in 2023 to combat financial cybercrime, including online fraud and money laundering. This operation helped recover $130 million stolen from victims of cyberattacks in 25 countries. [2]

In 2023, Interpol expanded its Cyber Fusion Centre to analyze and coordinate cybercrime. The centre has become a platform for law enforcement, private companies and cybersecurity experts to collaborate. This allows for rapid identification of cyber threats and real-time response.

Ransomware remains a serious problem in cyberspace, and Interpol is actively combating these threats. As part of the initiative to stop ransomware, Interpol works with the private sector and governments to monitor the activities of criminal groups. The organization also helps victims decrypt encrypted data by providing them with access to data recovery keys. [3]

One of Interpol's priorities for 2023-2024 is the fight against illegal activities on the Darknet. Interpol, together with police and customs authorities, conducted operations to identify and apprehend members of criminal networks involved in the trade of drugs, weapons and counterfeit documents on the Darknet. This activity includes the use of special tools to analyze cryptocurrency transactions and monitor activity on Darknet platforms. [4]

Europol also actively cooperates with the European Union and its member governments to identify and neutralize threats in the information space. The organization organizes joint operations and provides expertise for investigations. For example, in 2020, Europol participated in a joint operation against botnets used to attack financial institutions around the world. [5]

In 2023-2024, Europol actively fought transnational crime in the field of information technology, organizing various operations and initiatives. In particular, the 2023 operation “EMMA8” was aimed at combating fraud through email and banking schemes. The organization cooperated with more than 20 state and financial institutions to identify criminal groups and prevent cyberattacks.

Europol pays particular attention to combating ransomware attacks, which pose a serious threat to businesses and public institutions. In 2023, Europol successfully carried out Operation “Quicksand”, aimed at disrupting the infrastructure used by ransomware groups. Europol is expanding its cooperation with technology companies and financial institutions in the fight against IT crime. As part of the “No More Ransom” initiative, Europol is joining forces with private companies to help victims of ransomware. The “No More Ransom” initiative website provides free tools for encrypting data, helping to prevent millions of euros in losses. [6]

In 2023-2024, Europol is actively coordinating efforts to neutralize botnets and take down their control servers in the fight against DDoS (Denial of Service) attacks. In addition, it will coordinate joint efforts to prevent illegal crypto payments associated with ransomware and black market trading in a number of countries. [7]

The United Nations Office on Drugs and Crime (UNODC) is developing and implementing global initiatives to strengthen cybersecurity in countries with low levels of security. In particular, it conducts training and seminars for government agencies and law enforcement agencies around the world to increase their capacity to combat cybercrime. [8] In 2024, new guidelines were published for countries to introduce effective legal and enforcement mechanisms.

The UN Office on Drugs and Crime will conduct advocacy to raise awareness among citizens and organizations about cyberthreats, including educational materials and learning resources. In 2024, the main focus will be on preventing young people from getting involved in cybercrime. [9]

In recent years, the Financial Action Task Force (FATF) has also been actively working to combat transnational crimes in the field of information technology, in particular, money laundering and terrorist financing. [10] This group focuses on introducing innovative solutions to increase the effectiveness of measures to combat money laundering and terrorist financing. This includes the use of technology to process data, analyze it collaboratively, and improve data security. Despite the activities of authoritative international organizations to combat transnational crimes in the field of information technology, combating crime in the digital space is becoming increasingly difficult. First, the problem of combating such crimes is complicated by their global nature, with criminals located in one country and their victims located in another. This requires coordinated action at the international level. [11]

One of the main challenges for international cooperation in combating crime in this area is the differences in national legislation. [12] This applies both to the interpretation of legislation and to approaches to regulating the digital environment. For example, laws on crimes in the field of information technology or cybercrime can vary greatly in many countries. Some countries have strict laws against online hacking and fraud, while others may not strictly regulate these crimes.

In addition, differences in approaches to data protection also create serious obstacles to international cooperation. [13] The European Union has a General Data Protection Regulation, which imposes strict restrictions on the transfer of personal data outside the European Union. Other countries (Nigeria, Cambodia, Laos, Myanmar, Venezuela, Bolivia) do not have similar standards, especially in countries that do not have strict data protection laws. [14] This creates difficulties for law enforcement agencies that need to exchange information when investigating transnational crimes.

Conclusion.

Another important problem in combating transnational crimes in the field of information technology is the technological disparity between countries. The development of information technology infrastructure varies depending on the economic and technological capabilities of countries, which leads to significant differences in their ability to effectively combat threats. Developing countries often do not have sufficient resources to create effective cybersecurity systems and ensure the necessary level of training.

Countries with a low level of technological development often do not have the necessary information technology infrastructure, which makes them vulnerable to cyberattacks. Criminals can use these countries as a platform for conducting cyberattacks on other countries. Because weak security infrastructure makes it difficult to detect threats in a timely manner. In such cases, criminals can escape criminal responsibility due to geographical barriers and ineffective law

enforcement in those countries. In addition, it is worth noting the problem of a shortage of qualified personnel in the field of cybersecurity. Developing countries face a shortage of specialists who can effectively protect their IT infrastructure from threats, which creates an additional barrier to cooperation with developed countries.

REREFENCES

1. 1.Top Cybersecurity Statistics for 2024 // https://www.cobalt.io/blog/cybersecurity-statistics-2024
2. USD 300 million seized and 3,500 suspects arrested in international financial crime operation // https://www.interpol.int/News-and-Events/News/2023/USD-300-million-seized-and-3-500-suspects-arrested-in-international-financial-crime-operation
3. Top Cybersecurity Statistics for 2024 // https://www.cobalt.io/blog/cybersecurity-statistics-2024
4. 300+ Terrifying Cybercrime and Cybersecurity Statistics (2024 EDITION) // https://www.comparitech.com/vpn/cybersecurity-cyber-crime-statistics-facts-trends/
5. USD 300 million seized and 3,500 suspects arrested in international financial crime operation // https://www.interpol.int/News-and-Events/News/2023/USD-300-million-seized-and-3-500-suspects-arrested-in-international-financial-crime-operation
6. 115 cybersecurity statistics + trends to know in 2024 // https://us.norton.com/blog/emerging-threats/cybersecurity-statistics
7. International Investigation Leads to Shutdown of Ransomware Group // https://www.fbi.gov/contact-us/field-offices/cleveland/news/international-investigation-leads-to-shutdown-of-ransomware-group
8. UNODC. (2024). "Legislative Frameworks for Cybercrime." UNODC Legislative Frameworks.
9. FATF (2021), Opportunities and Challenges of New Technologies for AML/CFT, FATF, Paris, France, https://www.fatf-gafi.org/publications/fatfrecommendations/documents/opportunities-challenges-newtechnologies-aml-cft.html
10. Urgent cooperation needed to fight money laundering and terrorist financing // https://www.interpol.int/News-and-Events/News/2024/Urgent-cooperation-needed-to-fight-money-laundering-and-terrorist-financing
11. Digital Transformation of AML/CFT // https://www.fatf-gafi.org/en/publications/Digitaltransformation/Digital-transformation.html
12. Urgent cooperation needed to fight money laundering and terrorist financing // https://www.interpol.int/News-and-Events/News/2024/Urgent-cooperation-needed-to-fight-money-laundering-and-terrorist-financing
13. Opportunities and Challenges of New Technologies for AML/CFT // https://www.fatf-gafi.org/en/publications/Digitaltransformation/Opportunities-challenges-new-technologies-for-aml-cft.html
14. Digital Transformation of AML/CFT // https://www.fatf-gafi.org/en/publications/Digitaltransformation/Digital-transformation.html