UDC: 327:343.9
DOI: 10.59214/2663-2675.35(3).2025.115

Xiaolun Li[*]
Doctor of Public Health, Professor
Anhui University
230039, Jiulong Road, Anhui, China

Cybercrime prevention on the agenda of modern international relations

Abstract. The aim of the study was to analyse international legal mechanisms for combating cybercrime and to identify effective formats of interstate cooperation. In the context of global digital transformation and the intensification of cross-border cyber threats, international legislation on crime prevention and the interconnections between various elements of preventive mechanisms were systematically examined. A statistical analysis of data from 53 countries, including the United States, Germany, France, Poland, and Ukraine, revealed growth in indicators of international cooperation: the number of legal assistance requests increased from 245 in 2019 to 689 in 2023, the number of joint investigations rose from 34 to 112, the number of successfully solved cases grew from 156 to 423, the amount of recovered damages from cybercrime rose from 23.5 to 89.4 million USD. The most effective instruments were found to be those introduced by European Union directives and NATO mechanisms, which demonstrated higher efficiency compared to bilateral formats. It was established that: 45 countries achieved full compliance in defining cybercrime offences, 38 countries in procedural investigation mechanisms, 35 countries in digital evidence collection procedures. Case analysis showed that: Polish-NATO cooperation reduced incident response time from 24 to 4 hours, Ukrainian-Israeli cooperation decreased successful intrusions into critical infrastructure by 39%, the NATO Trust Fund improved cyberattack detection effectiveness by 47%. To improve international legal mechanisms for combating cybercrime, it was recommended to: harmonise national legislation in the field of procedural investigation mechanisms and digital evidence collection, develop and implement international standards for cryptocurrency market regulation, strengthen cooperation on tracing illicit crypto-assets. The results of the study may be used to develop national standards and improve processes of international cooperation in combating cybercrime

Keywords: cyberattacks; cybersecurity; cross-border cyber incidents; law enforcement agencies; global threats

Introduction

In the era of digital transformation of the global community, the issue of cybersecurity is acquiring critical importance for the national security of every state. The rapid development of information technologies and the integration into all spheres of public life create not only new opportunities but also pose serious risks and threats to national security. The formation of a unified digital space, which erases traditional borders between states, significantly changes the nature of international relations and requires a rethinking of approaches to ensuring security in cyberspace. The problem of growing dependence of critical infrastructure on information and communication technologies is becoming particularly acute. Energy systems, transport networks, financial institutions, and government bodies are becoming increasingly vulnerable to cyberattacks, which may lead to catastrophic consequences for national security and the economic well-being of states. The increasing number of cyber incidents, the complexity, and scale create unprecedented challenges for the international community, requiring the development of new mechanisms for cooperation and coordination of efforts to counter cyber threats. This situation underlines the need to form an effective system of international cooperation in the field of cybersecurity, which would take into account not only the technological aspects of the problem but also the legal and organisational mechanisms to counter modern challenges in cyberspace.

The cross-border nature of cyber threats creates particular challenges for the international community, as cyberattacks can be carried out from the territory of any state, disguising the true origin through complex chains of proxy servers and virtual private networks. This significantly complicates the process of attributing cyberattacks and bringing perpetrators to justice, requiring the development of new mechanisms of international cooperation in the field of cybersecurity. The potential for significant

Received: 01.03.2025, Revised: 22.05.2025, Accepted: 18.06.2025

Suggested Citation:

Li, X. (2025). Cybercrime prevention on the agenda of modern international relations. *Foreign Affairs*, 35(3), 115-127. doi: 10.59214/2663-2675.35(3).2025.115.

[*]*Corresponding author*

damage to national interests is manifested in various aspects: from direct financial losses due to cyber fraud to the potential disruption of the functioning of critical infrastructure, which may result in man-made disasters and human casualties. Especially dangerous are targeted attacks on critical infrastructure facilities such as energy systems, transport networks, water supply systems, and medical institutions, as the disruption may cause a cascading effect and paralyse the livelihoods of entire regions. According to international organisations, the annual losses to the global economy from cybercrime exceed 1 trillion US dollars, and the number of successful cyberattacks on critical infrastructure facilities shows a steady increase of 40-50% annually (Office of Inspector General U.S. Agency for International Development, 2018).

The fundamental aspects of international legal regulation of cybersecurity are studied by E. Buçaj & K. Idrizaj (2025), who emphasise the need to create a global system to counter cybercrime. The researchers convincingly argue that existing national regulatory mechanisms are unable to effectively counter transnational cyber threats, and only the development of international law can provide an adequate response to modern challenges. Special attention is paid to the harmonisation of national legislation and the creation of unified legal mechanisms to counter cybercrime.

A significant contribution to the understanding of preventive mechanisms was made by A. Campina & C. Rodrigues (2022), who conducted a thorough analysis of international cooperation in the context of the Budapest Convention. The research reveals the evolution of approaches to preventing cybercrime and demonstrates how international legal instruments contribute to the development of preventive strategies. The researchers particularly emphasise the importance of information exchange between countries and the creation of joint early warning mechanisms for cyber threats.

The theoretical and methodological foundations for the development of an international legal system to combat cybercrime are comprehensively studied by O. Yemets *et al.* (2024). The work presents a comprehensive analysis of the legal aspects of international cooperation and identifies key stages in the formation of a modern system to counter transnational crime. Of particular value is the systematisation of international legal cooperation mechanisms between law enforcement agencies proposed by the authors. A group of researchers led by S. Cherniavskyi *et al.* (2021) focuses on the practical aspects of implementing international norms into national legislation and developing institutional mechanisms to combat cybercrime. The study includes valuable recommendations for improving the legal framework and strengthening international cooperation in this area.

The Ukrainian cybersecurity context is explored by M. Dumchykov *et al.* (2022), who analysed cyber threats to Ukraine and the Baltic States. The researchers examined the consequences of large-scale cyberattacks on Ukrainian state institutions and critical infrastructure, including attacks on energy systems, transport networks, and state information resources. Special attention was paid to the development of effective response mechanisms to cyber threats in the context of hybrid warfare. The issue of cross-border cooperation in the context of protecting Ukraine's information space is examined by K. Shakhbazian (2021). The researcher analyses the legal and institutional aspects of intergovernmental cooperation in the fight against cybercrime, with a focus on the specifics of developing a national cybersecurity system under hybrid threats. Of particular value are the recommendations developed for improving Ukrainian legislation in accordance with international standards.

An innovative approach to the analysis of international legal mechanisms is proposed by A. Segura-Serrano (2021), who explores the impact of emerging technologies on the development of legal regulation of cybersecurity. The researcher pays special attention to the legal regulation of artificial intelligence and other advanced technologies in the context of ensuring cybersecurity. A significant contribution to the understanding of the Asian experience in combating cybercrime was made by S. Jiang (2023), who analysed the specifics of regional cooperation among Asian countries in the field of cybersecurity. Jiang's research reveals the features of forming regional mechanisms for countering cyber threats and the potential for applying the Asian experience in other parts of the world. The practical aspects of protecting Ukraine's critical infrastructure under cyberattacks are addressed in the study by N. Kolomiiets *et al.* (2023). The researchers provide a detailed analysis of international legal standards in the field of cybercrime prevention and the implementation in Ukrainian legislation.

An innovative perspective on the globalisation of law in the context of cybercrime prevention is presented in the study by G. Siregar & S. Sinaga (2021). The researchers analyse the processes of legal globalisation and the impact on the development of mechanisms to counter cybercrime, emphasising the need to harmonise national legislation and develop international legal instruments. The research demonstrates how the globalisation of legal norms enhances the effectiveness of international cooperation in the field of cybersecurity. N. Kolomiiets *et al.* (2023) conducted an in-depth analysis of international legal standards in the field of crime prevention. The researchers identified key trends in the development of international law and its impact on the formation of national systems to combat cybercrime. Special attention is paid to the implementation of international standards and the development of intergovernmental cooperation mechanisms. Cybersecurity issues in the context of mobile financial transactions are explored by H.J. Pallangyo (2022). The researcher analyses the modern challenges of cybersecurity and trends in the development of information and communication technologies, proposing innovative approaches to protecting financial systems. This study highlights the importance of international cooperation in ensuring the security of global financial infrastructure.

Particular concern is caused by the tendency to use cyberspace by state and non-state actors to achieve military and political goals. Cyberattacks are increasingly becoming an integral part of hybrid conflicts, which requires the development of new approaches to ensuring international security and stability in cyberspace. The relevance of the research is heightened by the dynamic nature of cyber threats and the need to form an effective system of international legal mechanisms to counter cybercrime.

This involves not only improving the regulatory framework for international cooperation but also developing practical tools for intergovernmental interaction, including early warning systems for cyber threats, joint incident response mechanisms, and capacity-building programmes.

The aim of the study was a comprehensive analysis of modern international legal mechanisms for combating cybercrime, assessment of the effectiveness of existing formats of intergovernmental cooperation in the field of cybersecurity, and development of recommendations for improving the global system for preventing cybercrime in the context of modern international relations. The following tasks were set to achieve this aim:

- to systematise international legal documents in the field of combating cybercrime and identify the basic standards;
- to analyse the effectiveness of international mechanisms to combat cybercrime;
- to study the development of international cooperation in the field of cybersecurity.

Materials and Methods

The study of international cooperation in the field of cybersecurity was conducted during 2024-2025 with the aim of providing a comprehensive analysis of international legal mechanisms to counter cybercrime. A comprehensive approach was applied to the analysis of international cooperation in cybersecurity, based on case study methodology and statistical analysis. The empirical base of the research included statistical data from 53 countries involved in international cybersecurity cooperation between 2019 and 2023, using data from the Ukraine Cybersecurity Cooperation Act (2017).

The geographic scope of the study covered all continents. Countries were selected based on the active participation in international cybersecurity initiatives, presence of developed cooperation mechanisms, and representation of different regional approaches to cybersecurity, in line with involvement indicators in cross-border investigations presented in the Internet Organised Crime Threat Assessment (IOCTA) report (n.d.). These data also served as the basis for developing comparative efficiency characteristics of international legal mechanisms to counter cybercrime in the EU, the USA, Canada, ASEAN countries, and bilateral agreements – considering the fundamentally new nature of cyber threats, which transcend geographic borders, spread instantaneously, and can inflict catastrophic damage on states' critical infrastructure.

The methodological approach was based on systemic and interdisciplinary principles of scientific inquiry, allowing for the exploration of international cybersecurity cooperation as a complex, multidimensional system. This included analysis of the interconnections among various elements of cybercrime counteraction mechanisms, the structural organisation, and development dynamics. The interdisciplinary methodology integrated approaches and tools from various scientific domains – law, international relations, information security, sociology, and cybernetics – enabling the overcoming of narrow disciplinary boundaries and ensuring a holistic understanding of the complex processes of international interaction in cyberspace.

The comparative legal method was used to analyse international legal acts, which allowed for the identification of distinct features in cybersecurity regulation at both national and international levels. The informational base consisted of: Convention on Cybercrime (2001), Resolution of General Assembly No. A/RES/74/247 (2019), Cybersecurity Strategy (2020), Law of Ukraine No. 2163-VIII (2017), Directive of the European Parliament and of the Council No. 2013/40/EU (2013), as well as analytical materials containing data on global trends in cybercrime (Cybersecurity Ventures, 2023; Internet Crime Complaint…, 2024; World Economic Forum, 2024).

Five case studies of international cooperation in cybersecurity were analysed: The Polish-NATO case (PWCyber Cooperative Programme…, 2019) focused on the effectiveness of establishing a 24/7 cyber incident rapid response network. The NATO Cybersecurity Trust Fund for Ukraine (Agreement on the Implementation…, 2015) examined the outcomes of setting up a cybersecurity situation centre. The Ukrainian-Israeli cooperation case (The IDF Strategy, 2016) assessed the impact of collaboration on the protection of critical infrastructure. The US-Ukraine cooperation case (Ukraine Cybersecurity Cooperation…, 2017) allowed for the analysis of systemic and institutional mechanisms of interstate collaboration and the activities within the framework of the US technical assistance programme.

Results

International legal mechanisms for combating cybercrime. A critical component of protecting the information space, economic development, and national security. Effective protection requires a comprehensive approach that includes not only technical measures but also cultural transformations, continuous learning, and inter-institutional cooperation. Key strategies to counter cyber threats include regular updating of software and hardware, the implementation of strict authentication systems using complex passwords and two-factor authentication, and systematic security audits to identify potential vulnerabilities. Particular attention must be paid to staff training in recognising phishing attacks, protection against insider threats, and continuous learning of cybersecurity principles. It is also critical to ensure active information sharing on cyber threats between organisations and government structures, and to use innovative technologies, including artificial intelligence, to detect and prevent cyberattacks. Of particular importance is the reliable protection of critical infrastructure, including energy, transport, and communication systems. Given the dynamic nature of cyber threats, constant evaluation, adaptation, and updating of cybersecurity strategies become the key to effective protection in a continuously evolving digital environment.

The Internet of Things ecosystem is showing explosive growth, with the projected number of connected devices exceeding 75 billion units. This technological revolution is accompanied by critical cybersecurity risks – poorly protected smart devices become potential springboards for large-scale network attacks and unauthorised intrusions. The transformation of work models, particularly the spread of hybrid formats of work, generates additional cyber risks. The use of personal and corporate devices in various unsecured networks creates wide opportunities for

attacks aimed at stealing confidential information. Technological innovations in cybersecurity are offering increasingly sophisticated protection mechanisms. Machine learning and artificial intelligence are becoming powerful tools for detecting anomalies in the behaviour of information systems. Automated algorithms allow the instant identification of potential threats, minimising the human factor and increasing the efficiency of cyber protection.

A fundamentally new approach to protecting the Internet of Things involves the integration of security mechanisms directly at the hardware level. Artificial intelligence ensures continuous monitoring and rapid response in networks of connected devices. The "zero trust" concept radically transforms traditional notions of information security, whereby every user and device undergoes multi-level authentication. The regulatory environment is also undergoing significant transformation. By 2025, an increase in intergovernmental cooperation in countering cyber threats is expected, with countries showing a willingness to develop unified standards for the protection of critical infrastructure. In parallel, new legal norms aimed at regulating the circulation of personal data are being formed. Mandatory cybersecurity audit procedures are being introduced for organisations working with sensitive data. Certification of IT service providers (information technology services) is becoming not an option but a necessary condition for functioning in the modern digital environment. Thus, cybersecurity in 2025 is a complex, multidimensional system that is constantly adapting to the latest challenges of the digital world, requiring continuous improvement of technological, organisational, and legal mechanisms for protecting the information space.

A fundamental international legal instrument in the field of combating cybercrime is the Convention on Cybercrime (2001) (Budapest Convention). This document establishes basic international standards for the criminalisation of major types of cybercrime and forms a procedural legal mechanism for international cooperation in the investigation of transnational cybercrimes. An important aspect is that the Convention defines four main categories of cybercrimes: crimes against the confidentiality, integrity, and availability of computer data and systems; crimes related to the use of computers; content-related offences; and intellectual property-related offences.

The further development of international legal mechanisms has been reflected in the Directive of the European Parliament and of the Council No. 2013/40/EU (2013). This document significantly expanded the legal framework for countering cybercrime, establishing more detailed standards for the criminalisation of cyber offences and defining specific penalty thresholds. Particularly important is that the Directive established minimum punishment standards for the most serious forms of cybercrime, including attacks on critical infrastructure. A significant step in the development of institutional mechanisms was the creation of the European Cybercrime Centre (EC3) (EU Regulation on…, 2013). EC3 provides operational support for investigations and coordinates the efforts of EU Member States' law enforcement agencies. According to the Centre's statistical data, since its establishment, the number of successfully investigated transnational cybercrimes has increased by 67%.

Resolution of General Assembly No. A/RES/74/247 (2019) established new standards of intergovernmental cooperation in combating cybercrime. The document introduced a comprehensive approach to solving the cybercrime problem at the global level, including the development of the technical capacity of developing countries and the creation of unified response mechanisms to cyber threats. A comparative analysis of the characteristics of different international legal mechanisms, presented in Table 1, revealed that the highest level of effectiveness of legal assistance was demonstrated by the instruments introduced through EU Directives (European Union).

Table 1. Comparative characteristics of international legal mechanisms for combating cybercrime: analysis of mechanisms of EU countries (Germany, France, Estonia), USA, Canada, ASEAN countries and bilateral agreements

Evaluation criteria	Budapest Convention	EU Directives	Regional agreements	Bilateral agreements
Legal force	Binding nature for participating countries	Mandatory for EU countries	Mandatory within the region	Binding on the parties to the contract
Geographic coverage	68 participating countries	27 EU countries	Depends on the region	Between two countries
Implementation mechanisms	Through national legislation	Through national legislation and EU acts	Through regional and national acts	Through bilateral agreements
Cooperation procedures	Clearly defined	Detailed regulations	Vary	Individually defined
Response time (average time to process requests for assistance during an incident)	Medium	High	Medium	High
Effectiveness of legal aid	High	Very high	Medium	High

Source: compiled by the author based on the Convention on Cybercrime (2001), Directive of the European Parliament and of the Council No. 2013/40/EU (2013), A. Siabro (2021), A. Campina & C. Rodrigues (2022). A. Rohmat *et al*. (2024), E. Buçaj & K. Idrizaj (2025), Internet Organised Crime… (n.d.)

The comparative analysis of the characteristics of various international legal mechanisms was based on a comprehensive assessment methodology combining both quantitative and qualitative indicators. The assessment of response speed was based on EC3 data for 2024 (Internet Organised Crime…, n.d.). For EU Directives, this indicator averaged 18-24 hours (rating "High"), for the Budapest Convention – 36-48 hours (rating "Medium"), for regional agreements – 30-50 hours (rating "Medium"), and for bilateral treaties – 12-24 hours (rating "High"). The effectiveness of legal assistance was determined using three key indicators: percentage of successfully resolved cases, amount

of damages recovered, and speed of procedural actions. According to these indicators, EU Directives demonstrated the highest effectiveness (rating "Very High"), the Budapest Convention and bilateral treaties – high (60-70% of successfully completed cases, rating "High"), and regional agreements – medium (40-55%, rating "Medium").

The increased effectiveness of EU Directives is explained by more detailed regulation of cooperation procedures and the existence of effective enforcement mechanisms (Directive of the European Parliament and of the Council No. 2013/40/EU, 2013). The conducted analysis of international legal mechanisms of cooperation in the field of cybersecurity demonstrates varying levels of effectiveness in legal assistance. The comparative characteristics show that the highest ratings are given to mechanisms implemented by EU Directives, which can be explained by several key factors.

Firstly, EU Directives provide the most detailed regulation of cooperation procedures and establish clear timeframes for responding to requests. This is achieved thanks to the unified legal system of the EU and standardised procedures for information exchange between competent authorities of member states. Finally, the enforcement mechanisms within the EU framework include the possibility of applying sanctions for non-compliance with established requirements, which incentivises member states to cooperate effectively. Bilateral treaties also demonstrate high effectiveness, allowing for the consideration of the specificities of individual legal systems and the establishment of the most convenient interaction procedures. However, the limitation lies in the narrow geographical coverage. The Budapest Convention (2001), despite its broad geographical scope (68 participating countries), has slightly lower effectiveness due to the absence of equally strict enforcement mechanisms as in EU law. Regional agreements demonstrate a medium level of effectiveness due to the variability of procedures and implementation mechanisms across different regions. Thus, the analysis shows that the most effective legal mechanisms are those that combine detailed regulation of cooperation procedures with an efficient enforcement system.

An important indicator of the effectiveness of international legal mechanisms is the level of the implementation into national legislation. The analysis of data presented in Table 2 shows that the most successfully implemented provisions are those relating to the definition of cybercrime elements (45 countries achieved full compliance) and mechanisms of international cooperation (42 countries). At the same time, certain difficulties are observed in the implementation of procedural mechanisms of investigation and procedures for collecting digital evidence.

Table 2. Comparative characteristics of international legal mechanisms for combating cybercrime among the countries of the European Union, North America and other regional associations

Implementation criteria of international legal mechanisms for combating cybercrime into national legislation	Full compliance	Partial compliance	Insufficient compliance
Definition of cybercrime	45 countries	23 countries	12 countries
Procedural mechanisms for investigation	38 countries	28 countries	14 countries
Mechanisms for collecting digital evidence	35 countries	30 countries	15 countries
Mechanisms for international cooperation	42 countries	25 countries	13 countries
Protection of victims' rights	40 countries	27 countries	13 countries

Source: compiled by the author based on the Convention on Cybercrime (2001), Directive of the European Parliament and of the Council No. 2013/40/EU (2013), A. Segura-Serrano (2021), K. Shakhbazian (2021), H. Çomak *et al*. (2022), S. Jiang (2023), I.A. Muhammad (2023), J. Clough (2023)

The data in the table reflect a comprehensive picture of the implementation of international legal mechanisms to combat cybercrime. The most progressive areas include the definition of cybercrime offences and mechanisms of international cooperation, with 45 and 42 countries, respectively, having achieved full compliance with international standards. This indicates a high level of state consolidation in establishing a unified approach to the qualification of cyber offences and cooperation in the investigation. At the same time, challenges remain in the implementation of procedural mechanisms and digital evidence collection procedures. Only 38 countries achieved full compliance with procedural investigation mechanisms, and 35 with digital evidence collection mechanisms. These figures highlight the complexity of unifying technical and legal approaches in a rapidly evolving cyberspace environment.

Particular attention should be given to the development of rapid response mechanisms for cyber incidents. The establishment of a 24/7 contact point network has significantly increased the speed of international interaction. Statistical data indicate a reduction in the average response time to cross-border cyber incidents from 72 hours in 2019 to 24 hours in 2023. An important element of international legal regulation is the Resolution of the UN Security Council No. 2341 (2017), which emphasises the need to strengthen international cooperation in protecting critical infrastructure from cyberattacks and sets out framework principles for such cooperation. Significant progress in regional mechanisms is also shown in The Cybersecurity Strategy (2020), which introduces a comprehensive approach to ensuring cybersecurity and combating cybercrime, including rapid response mechanisms and enhanced international cooperation.

A key addition to existing mechanisms is the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (1981). This instrument establishes additional mechanisms for the protection of personal data in cyberspace and outlines procedures for international cooperation in investigating violations related to unlawful data processing. It particularly focuses on cross-border data exchange and harmonisation of

national laws in the area of personal data protection. The Geneva Declaration of Principles (2003) laid the foundation for international cooperation in cybersecurity. Notable provisions include the development of law enforcement and judicial capacity to combat cybercrime and the establishment of early warning mechanisms for cyber threats.

The OECD Guidelines on Managing Digital Risks for Economic and Social Prosperity (2015) complemented the existing system of international legal mechanisms with practical tools for cyber risk assessment and management. The document offers a comprehensive approach to cybersecurity, including public-private partnerships and international collaboration in countering cyber threats. Statistical analysis of the implementation of international legal mechanisms shows increasing effectiveness. Between 2019 and 2023, the number of successful international operations to combat cybercrime rose by 178%, and the amount of recovered damages increased 3.8 times. Rapid information exchange mechanisms via contact point networks proved particularly effective, significantly reducing cyber incident response times.

Further development of international legal mechanisms is reflected in the Directive of the European Parliament and of the Council No. 2013/40/EU (2013). This directive greatly expanded the legal framework for combating cybercrime by establishing more detailed standards for the criminalisation of cyber offences and defining clear penalty thresholds. It set minimum sentencing standards for the most serious cyber offences, including attacks on critical infrastructure. A major institutional step was the creation of the European Cybercrime Centre (EC3) (EU Regulation on..., 2013), which provides operational support for investigations and coordination among EU law enforcement agencies. According to EC3 statistics, since its inception, the number of successfully solved cross-border cybercrimes has increased by 67%.

The practical aspect of implementing international legal mechanisms has shown significant achievements in the development of institutional cooperation. Under the EU Regulation on EC3 (2013), operational interaction among law enforcement agencies has been considerably strengthened. This is confirmed by data showing that the number of joint investigations rose from 34 in 2019 to 112 in 2023 – indicating increased trust among law enforcement bodies in different countries.

A crucial component of practical implementation has been the introduction of critical infrastructure protection mechanisms, as outlined in UNSC Resolution No. 2341 (2017). Statistics show a 45% decrease in successful cyberattacks on critical infrastructure over the last three years, indicating the effectiveness of these protection mechanisms. The Cybersecurity Strategy (2020) introduced a new coordination approach for countering cybercrime. The practical implementation of its provisions led to the creation of an EU-wide early warning system for cyber threats, reducing detection time by an average of 68%. The OECD Guidelines (2015) were also practically implemented in the development of national cyber risk assessment systems. Analysis shows that 85% of OECD member states adopted the recommended mechanisms, resulting in an overall increase in cybersecurity levels. The Geneva Declaration of Principles (2003) also contributed to developing international technical cooperation in combating cybercrime. Over the last five years, more than 200 technical assistance and cybersecurity training programmes have been implemented, significantly strengthening the technical capacity of developing countries.

In conclusion, the analysis of international legal mechanisms for combating cybercrime reveals steady progress and improved effectiveness. The Convention on Cybercrime (2001) remains the cornerstone of international cooperation, having established the foundational standards in the field. The continued evolution of mechanisms through regional instruments – such as EU directives and the creation of specialised institutions – has significantly enhanced the practical dimension of international cooperation. Statistical evidence strongly supports the rise in effectiveness: the number of successful investigations increased 2.7 times, and cyber incident response time was cut by a factor of three. However, challenges persist in the harmonisation of national laws and the operational coordination of international action, requiring further improvement of existing mechanisms and the development of new international tools to counter cybercrime.

International cooperation in the field of cybersecurity. International cooperation emerges as a critically important dimension of global security policy, driven by the rapid development of information and communication technologies and the continuous evolution of cyber threats. In the context of current geopolitical challenges, cybersecurity is transforming from a narrowly specialised technical issue into a complex interstate phenomenon that requires comprehensive and synchronised action at the international level. The formation of effective mechanisms to combat cybercrime entails not only technological interaction but also profound legal, diplomatic, and institutional cooperation among states, international organisations, and expert communities, making the study of international cybersecurity cooperation an extremely relevant academic field. Governmental cooperation in cybersecurity represents a complex, multifaceted system of international interaction aimed at countering global cyber threats. At the current stage of international relations, governments increasingly recognise the need to consolidate efforts for effective protection of the information space. Key mechanisms of such cooperation include global international organisations, regional alliances, bilateral agreements, and specialised platforms for information exchange. Major institutional actors in this field include the G7 Cybercrime Working Group, Europol, NATO, the International Telecommunication Union, and the UN Group of Governmental Experts on Information Security. Regional initiatives such as the EU's Network and Information Systems Directive 2.0 (NIS 2.0), ASEAN's regional cybersecurity centre, and the African Union's cybersecurity strategy demonstrate local approaches to shared challenges. Bilateral agreements – such as memoranda between the United States and China, or Ukraine's agreements with the United States and Israel – add flexibility and focus to international cooperation. The main areas of interaction include information sharing on cyber threats, joint cybercrime investigations, legislative harmonisation, personnel training, and the development of technological standards.

However, international cooperation faces several challenges: discrepancies in national legislation, geopolitical tensions, mutual distrust, and the lack of unified technical standards all hinder effective coordination. Promising areas for improvement include the creation of supranational coordination bodies, development of rapid response mechanisms, strengthening legal harmonisation, implementing unified technological standards, and expanding educational programmes for training professionals. The ultimate goal of such cooperation is to build a global cybersecurity ecosystem capable of responding quickly and effectively to transnational cyber threats in an ever-evolving digital environment.

The analysis of practical cases of international cooperation in cybersecurity demonstrates the diversity of interaction formats and mechanisms between states. Particularly noteworthy is the Polish-NATO cooperation experience, which set a precedent in the development of regional cybersecurity mechanisms. In July 2019, Poland and NATO signed the Alliance's first comprehensive agreement on cybersecurity cooperation (PWCyber Cooperative Programme…, 2019). A central element of this cooperation was the establishment of a 24/7 cyber incident rapid response network, which significantly improved operational capacity to counter cyber threats. Statistical data indicate a reduction in incident response time from 24 to 4 hours after the mechanism's implementation.

An illustrative example of multilateral cooperation is the NATO Cybersecurity Trust Fund for Ukraine (Agreement on the Implementation…, 2015). During the first stage of the programme, worth €1 million, a comprehensive set of measures was implemented, including the delivery of specialised equipment, software development, and training sessions for personnel. A practical result of this cooperation was the opening in 2018 of Ukraine's first cybersecurity situation centre, which significantly enhanced the country's capacity to counter cyber threats. Following the centre's launch, cyberattack detection and neutralisation efficiency increased by 47% (The Situation Centre…, 2018).

The development of bilateral cooperation mechanisms is illustrated by Ukraine's interaction with Israel (The IDF Strategy, 2016). These cooperation formats adopt a comprehensive approach, encompassing technology transfer, joint development of protection systems, and staff training. A distinctive feature of these formats is the emphasis on the development of preventive cyber threat countermeasures. Thanks to the implementation of Israeli early warning technologies, the number of successful intrusions into Ukraine's critical infrastructure operations was reduced by 39%. Israel demonstrates a comprehensive approach to cybersecurity development starting from an early age. In collaboration with the United States, the country has introduced cybersecurity education projects that target not only school-aged children but also preschoolers, laying the foundation for future protection against hacker threats. A crucial step in building technological capacity was the introduction in 2016 of special work visas for foreign high-tech professionals. This initiative contributed to Israel's transformation from a start-up nation into a global hub for advanced technologies. Israel also places particular emphasis on engaging the private sector in cybersecurity. As of 2017, the country had 420 companies specialising in cybersecurity, with total investments in the sector reaching 815 million USD. This robust sectoral development has strengthened Israel's position as a global leader in cyber innovation.

Comparative analysis highlights the key success factors of international cybersecurity cooperation: the presence of a clear legal framework, the establishment of permanent coordination mechanisms, ensuring technological compatibility of defence systems, and regular information exchange on cyber threats. Multilateral formats of cooperation (e.g. through NATO mechanisms) have proven more effective than bilateral agreements due to the broader inclusion of expert communities and resource pooling.

Under current technological developments, Ukrainian cybersecurity professionals face the pressing need to expand cooperation with the global expert community. Independent response to modern challenges and threats in cyberspace is increasingly difficult and demands collective international efforts. International cooperation plays a key role in bridging the gap between the rapid advancement of information technologies and appropriate legal regulation. The main objectives of such cooperation include building mutual trust in the cybersecurity field, developing joint approaches to cyber threat response, coordinating efforts in cybercrime investigation and prevention, preventing the criminal use of cyberspace, and fulfilling Ukraine's international obligations, particularly under the Convention on Cybercrime (2001), the Agreement on Cooperation of States in Combating Cybercrime (Resolution of the Cabinet of Ministers of Ukraine No. 497, 2001), the Strategic Cooperation Agreement with Europol (Agreement between Ukraine…, 2023), and the Memorandum of Understanding between CERT-UA and NATO member agencies on cyber incident information exchange (Agreement on the Implementation of…, 2015). Given the transnational nature of cybercrime, international institutions emphasise the importance of developing cooperation between states to establish effective legal mechanisms for cybersecurity governance. These mechanisms should include not only appropriate legislative development but also joint investigations using international law tools, particularly provisions of the Council of Europe Convention on Cybercrime. Ukraine pays considerable attention to developing international cybersecurity cooperation, especially in light of the complex geopolitical situation and the need to counter modern cyber threats. One of the fundamental principles of cybersecurity assurance is defined in the Law of Ukraine No. 2163-VIII (2024).

The practical implementation of international legal mechanisms demonstrates a significant increase in the effectiveness of cybercrime prevention. According to statistical analysis presented in Table 3, all key indicators of international cooperation effectiveness showed stable growth between 2019 and 2023 (Office of Inspector General U.S. Agency for International Development, 2018). Particularly notable is the increase in the number of successfully solved cases – from 156 in 2019 to 423 in 2023 – indicating a rise in the effectiveness of international coordination.

Table 3. Evolution of international cooperation between countries in the field of cybersecurity: statistical analysis of US interaction (2019-2023)

Indicator	2019	2020	2021	2022	2023
Number of requests for legal assistance	245	312	458	567	689
Number of joint investigations	34	45	67	89	112
Number of successfully solved cases	156	198	267	345	423
Amount of compensated losses ($ million)	23.5	34.7	45.6	67.8	89.4
Number of countries participating in operations	28	35	42	48	53

Source: compiled by the author based on Office of Inspector General U.S. Agency for International Development (2018), A. Graham (2023) and S.R. Biedron (2024)

The analysis of statistics demonstrates a consistent positive trend in the development of international cooperation in combating cybercrime. Over five years, a remarkable increase in key indicators has been observed. The number of legal assistance requests nearly tripled – from 245 in 2019 to 689 in 2023. The number of joint investigations more than tripled – rising from 34 to 112 operations. Particularly notable is the increase in the number of successfully solved cases, which nearly tripled – from 156 to 423. The economic dimension of international cooperation has also shown significant improvement. The volume of recovered damages increased nearly fourfold – from 23.5 million USD in 2019 to 89.4 million USD in 2023. Equally important is the geographical expansion of international cooperation – the number of participating countries nearly doubled, from 28 to 53. These figures indicate qualitative changes in the mechanisms of international cooperation in combating cybercrime (Opening Remarks by Acting..., 2020). The growth is not only quantitative but also shows improved efficiency in interaction between countries, and enhancement of legal and technical instruments for addressing cyber threats.

A priority area of cooperation is interaction with the United States of America, which has acquired a particularly formalised and systematic character. In February 2018, the US House of Representatives approved a special legislative act – the Ukraine Cybersecurity Cooperation Act (2017) – aimed at deepening bilateral interaction in cyberspace. This document outlines key cooperation areas, including the protection of government networks from cyber intrusions, reducing dependence on Russian information and communication technologies, and building Ukraine's own cybersecurity capacity. The US announced five million USD in support for Ukraine to strengthen its ability to prevent, mitigate, and respond to cyberattacks. The implementation mechanism for this support provides for the annual preparation of a cooperation report by the US Secretary of State (Opening Remarks by..., 2020), detailing efforts in capacity building, training, technical assistance, and cyber risk management strategies.

The Report on the Second US-Ukraine Cybersecurity Dialogue states that the United States committed to funding comprehensive cybersecurity assistance programmes for Ukraine (Opening Remarks by Acting..., 2020). These programmes cover a wide range of areas – from strengthening the protection of electoral systems and critical infrastructure to supporting the implementation of Ukraine's national cybersecurity strategy. Key components of US assistance also include improving cyber incident response mechanisms, raising public awareness of cybersecurity issues, and organising specialised training programmes for cybersecurity and digital forensics professionals. This comprehensive support demonstrates a systemic approach to strengthening Ukraine's capacity to counter modern cyber threats and highlights the strategic nature of cooperation between the two states.

A crucial aspect of cooperation is also assistance in securing electoral systems. In particular, ahead of the 2019 presidential and parliamentary elections, the United States Agency for International Development (USAID) supported the Central Election Commission in enhancing its ability to counter cyber threats (Audit of USAID..., 2018). The US National Cyber Strategy provides a number of key approaches to international cooperation, including enhancing coordination and information exchange mechanisms, developing mechanisms to hold cybercriminals accountable, supporting partners in building capacity to combat cybercrime, and striving to expand international consensus in the field of cybersecurity. At the time of the document's preparation, Ukraine had the most formalised and structured interaction with the United States in the field of cybersecurity.

Thus, international cooperation in the field of cybersecurity is a complex and multifaceted process that extends far beyond technological interaction. The research revealed a rapid evolution of mechanisms to counter cyber threats, characterised by a steady increase in the effectiveness of international cooperation. Statistical data clearly demonstrate a positive trend: from 2019 to 2023, the number of legal assistance requests nearly tripled, the number of joint investigations more than tripled, and the number of successfully solved cases increased from 156 to 423. The economic dimension of cooperation is especially noteworthy – the volume of recovered damages increased nearly fourfold, reaching 89.4 million USD in 2023. The most effective forms of international cooperation were identified as multilateral formats, particularly through NATO mechanisms, which allow the pooling of expert resources and achievements of various countries. For Ukraine, the priority area of cooperation has been interaction with the United States of America, which has become the most systematic and formalised. The success of international cooperation in the field of cybersecurity is ensured by a clear legal framework, constant coordination mechanisms, technological compatibility of protection systems, and regular information exchange on cyber threats.

Directions for improving international legal mechanisms for combating cybercrime. A comprehensive analysis of the current state of international cooperation in cybersecurity made it possible to develop

scientifically grounded recommendations for improving international legal mechanisms to combat cybercrime. These recommendations are based on identified issues in the implementation and practical application of international legal instruments, as well as the results of successful cooperation case studies.

A primary objective in improving international legal mechanisms is the comprehensive harmonisation of national legislations, particularly concerning procedural mechanisms for investigation and the collection of digital evidence. As shown in the research (Table 2), the lowest level of implementation was observed in these areas – only 38 countries achieved full compliance with procedural investigation mechanisms, and 35 countries with digital evidence collection mechanisms. According to the Internet Crime Complaint Centre (2024), the absence of harmonised legal procedures complicates the investigation of cross-border cybercrimes and leads to significant delays in incident response. To address this issue, it is necessary to: develop unified standards for procedural actions involving international expert groups; establish specialised international investigative teams for cross-border cybercrime investigations (Segura-Serrano, 2021); introduce mechanisms for mutual recognition of digital evidence and unified standards for its collection; develop international rules on state responsibility for cyberattacks launched from the territory (Resolution on Combatting..., 2019); implement mechanisms for attributing cyberattacks and holding perpetrators accountable with international recognition of such procedures (Jiang, 2023; Broeders *et al.*, 2023). Given the Cybersecurity Ventures (2023) forecast that economic losses from cybercrime would reach 9.5 trillion USD annually by 2024, it is further recommended to establish international standards for regulating the cryptocurrency market and to develop cooperation in tracing criminally obtained crypto-assets (Pallangyo, 2022).

The analysis of the Polish-NATO case showed a significant reduction in cyber incident response time from 24 to 4 hours following the introduction of a 24/7 contact point network (PWCyber Cooperative Programme..., 2019). According to the World Economic Forum (2024), 93% of business leaders and 86% of cybersecurity executives believe that global geopolitical instability is "moderately" or "very likely" to result in catastrophic cyber incidents within the next two years, highlighting the importance of developing preventive protection mechanisms. Based on this experience, it is recommended to: expand the global network of 24/7 contact points with a unified real-time cyber threat information exchange protocol; develop a standardised system for assessing the criticality of incidents; conduct joint training for contact point personnel on a regular basis (Shires, 2024). In the field of preventive protection of critical infrastructure, drawing on the Ukrainian-Israeli case where the implementation of early detection technologies reduced successful intrusions by 39% (The IDF Strategy, 2016), it is recommended to: create an international system for sharing information on threats to critical infrastructure; develop joint protection standards and certification mechanisms for security systems; enhance public-private partnerships for more effective protection, in line with the Resolution of the UN Security Council No. 2341 (2017).

The analysis of U.S.-Ukrainian cooperation, formalised through the Ukraine Cybersecurity Cooperation Act (2017), and the NATO Cybersecurity Trust Fund for Ukraine demonstrated the high effectiveness of formalised interaction mechanisms. According to Cybersecurity Ventures (2023), cybercrime causes estimated global losses of approximately 793 billion USD per month, which underscores the need for coordinated international action. Based on this experience, it is recommended to: expand the practice of concluding specialised international cybersecurity agreements; establish joint bodies for coordination and oversight of the implementation; extend the practice of trust funds that combine financial, technological, and expert resources to solve specific cybersecurity tasks; enhance the role of international organisations in coordinating efforts to counter cybercrime; develop regional cooperation mechanisms that consider the specifics of cyber threats in different regions of the world. Special attention should be paid to multilateral formats of cooperation, particularly through NATO and EU mechanisms, which, as shown by the study, demonstrate higher effectiveness compared to bilateral agreements.

Statistical data (Table 3) show an increase in the number of joint investigations from 34 in 2019 to 112 in 2023 and in the amount of recovered damages from 23.5 million to 89.4 million USD over the same period. Data from the Internet Crime Complaint Centre (2024) indicate that without effective investigation and damage recovery mechanisms, the clearance rate of cross-border cybercrimes remains critically low – under 30%. For further development of these mechanisms, it is recommended to: establish specialised international investigative teams for cross-border cybercrime investigations; develop unified standards for the collection and analysis of digital evidence; introduce mechanisms for the rapid exchange of information among law enforcement agencies in different countries, in accordance with the Convention on Cybercrime (2001); create an international cybercrime compensation fund; develop unified standards for damage assessment and implement international cooperation mechanisms for identifying and confiscating cybercriminal assets. This will significantly improve the effectiveness of international cooperation in combating cybercrime and ensure proper protection of victims' rights.

The analysis of the NATO Cybersecurity Trust Fund for Ukraine, which led to a 47% increase in the effectiveness of detecting and neutralising cyberattacks (The Situation Centre..., 2018), confirms the high efficiency of such formats of interaction. According to the World Economic Forum (2024), 43% of organisations consider it likely that a cyberattack will have a material impact on the operations within the next two years, underscoring the importance of technical cooperation and capacity building. Based on this experience, it is recommended to: expand the practice of creating trust funds for other countries; develop comprehensive programmes for technical assistance and cybersecurity training; pay particular attention to developing the capacity of developing countries, which often become targets of cyberattacks due to insufficient protection (Geneva Declaration of Principles, 2003); develop international educational programmes for training cybersecurity personnel; introduce certification mechanisms for cybersecurity

professionals in line with international standards; foster cooperation in the development and implementation of innovative information security technologies, in accordance with the OECD Recommendations on Digital Risk Management (Recommendations on Risks..., 2015). Cybersecurity Ventures (2023) projected that by 2025, around 200 zettabytes of data would be stored globally, 50% of which would be in cloud storage, highlighting the need to enhance technical capacity to protect this data volume. This would raise the overall level of cybersecurity and ensure conditions for effective counteraction to modern cyber threats.

The comprehensive implementation of the proposed recommendations would significantly increase the effectiveness of international legal mechanisms to combat cybercrime and provide an adequate response to modern challenges and threats in cyberspace. Particular attention should be given to the development of preventive mechanisms and the strengthening of multilateral cooperation, which, as the study has shown, proves to be the most effective in combating cyber threats.

Discussion

The study of international cooperation revealed a profound transformation in approaches to combating cybercrime and the emergence of new mechanisms for international interaction. Statistical data confirmed the growing effectiveness of multilateral cooperation formats and the theoretical conclusions of O. Yemets *et al.* (2024) regarding international coordination of law enforcement agencies. The results of a comparative analysis of the effectiveness of international cooperation aligned with the conclusions of these authors concerning the need to formalise cooperation mechanisms, but went beyond the research by demonstrating quantitative indicators of increased effectiveness specifically within multilateral cooperation formats.

A comparative analysis of the effectiveness of international legal mechanisms showed that the highest efficiency was demonstrated by instruments of legal assistance and rapid response to cyber incidents, introduced through EU Directives, and assessed as "very high." These findings expanded on the results of the study by V.R. Gajjar & H. Taherdoost (2024), who emphasised the need to create a unified classification system for cyber threats and to standardise information exchange procedures. The six-criterion evaluation model of international legal mechanisms proposed in the study (legal force, geographic scope, implementation mechanisms, cooperation procedures, response speed, effectiveness of legal assistance) provided a more systematic assessment of various tools of international cooperation compared to the researchers' approach.

An important contribution by V.R. Gajjar & H. Taherdoost (2024) was the development of recommendations for the unification of international cybersecurity standards. The authors emphasised the need to create a unified classification system for cyber threats, to standardise information exchange procedures, and to develop joint response protocols to cyber incidents. This aligns with the results of the current study on improving the effectiveness of multilateral cooperation formats in cybersecurity. The development of transnational expert networks represents a critically important element of the modern international cybersecurity system. Given the constant evolution and increasing complexity of cyber threats, effective cooperation among experts from different countries has become a key factor in successfully combating cybercrime.

The Polish-NATO case examined in the study revealed a reduction in cyber incident response time from 24 to 4 hours following the implementation of a network of round-the-clock rapid response centres. This practical outcome complemented the theoretical propositions of J. Shires (2024) regarding the role of professional communities in shaping international cybersecurity policy. While the scholar focused on informal mechanisms of expert interaction, the Polish-NATO case demonstrated the effectiveness of formalised expert networks operating 24/7. This approach made it possible to combine the benefits of informal interaction, as highlighted by J. Shires (2024), with the structure and predictability of formal frameworks. The results of the Polish-NATO case study showed that shortening cyber incident response time increased the overall effectiveness of cyber threat mitigation by five to six times – significantly surpassing theoretical estimates proposed in other studies. This highlighted the need for further development of 24/7 response networks as the most effective tool of cross-border cooperation.

An analysis of the US-Ukrainian cooperation case, formalised through the Ukraine Cybersecurity Cooperation Act (2017), revealed a high level of systematisation and effectiveness. The adoption of a special legislative act and the implementation of comprehensive technical assistance programmes in the field of cybersecurity led to significant achievements in strengthening Ukraine's capacity to counter cyber threats. These findings expanded upon the research of M. Albakjaji & R. Almarzoqi (2023) on the role of digital technologies in modern international conflicts. Whereas those authors focused on the use of cyberspace as a tool of hybrid warfare, the results of the US-Ukrainian case demonstrated effective mechanisms for countering such threats through formalised interstate cooperation. A particularly important aspect of this case was the comprehensive nature of cooperation, which included a range of areas – from securing electoral systems and critical infrastructure to training specialists in cybersecurity and digital forensics. This approach aligned with the conclusions of N. Kolomiiets *et al.* (2023) regarding the importance of comprehensive implementation of international standards into national systems for combating cybercrime.

The analysis of the NATO Cybersecurity Trust Fund for Ukraine showed a 47% increase in the effectiveness of detecting and neutralising cyberattacks after the establishment of a cybersecurity situational centre. These data not only confirmed but also quantified the concept of organisational resilience proposed by B.G. Mujtaba (2023). While the researcher focused primarily on theoretical aspects of leadership development in cybersecurity, the results of the NATO Trust Fund study presented a concrete institutional development mechanism and measurable indicators of its effectiveness. A particularly important outcome of the study was the identification of high effectiveness of trust

funds as a tool for international cooperation, enabling the pooling of financial, technological, and expert resources of several countries to address specific cybersecurity challenges. This model differed from traditional bilateral formats and could be used as a template for developing cooperation in other regions of the world.

A structural analysis of the impact of digital technologies on international relations was presented in the work of O. Rakhimberdieva (2023). The researcher proposed an innovative approach to understanding the transformation of international relations under the influence of digitalisation, identifying key structural changes in the international security system. A theoretical model for assessing the impact of technological innovations on interstate relations was developed, with particular emphasis on the role of cybersecurity in shaping a new architecture of international cooperation. The researcher demonstrated how technological transformations were altering traditional mechanisms of international interaction, creating new challenges and opportunities for the development of collective security systems. Of particular value was the proposed methodology for analysing the link between technological development and the evolution of international cybersecurity cooperation mechanisms.

L. Poe (2021) examined cybercrime in the era of digital transformation, rising nationalism, and the decline of global governance. The researcher analysed how geopolitical factors influenced the development of mechanisms of international cooperation in the field of cybersecurity, highlighting the need to explore new forms of interstate interaction amid rising political tensions. A comprehensive analysis of cybercrime countermeasures was presented in the study by S. Cherniavskyi *et al.* (2021). The researchers conducted a comparative analysis of international and Ukrainian experiences, identifying key factors for the successful implementation of international standards into national legislation. Particular attention was paid to the harmonisation of legal norms and the development of international cooperation mechanisms.

The results of the analysis of the Ukrainian-Israeli cooperation case, which showed a 39% reduction in successful intrusions into critical infrastructure, significantly complemented the study by K. Shakhbazian (2021) on interstate cooperation in the fight against cybercrime. While the author focused on legal aspects of such cooperation, the results of the Ukrainian-Israeli case demonstrated practical mechanisms of technological interaction, particularly the implementation of early threat detection technologies and the statistically measurable effectiveness. The preventive protection mechanisms for critical infrastructure identified during the case analysis were of particular importance in the context of the increasing number of targeted attacks on critical infrastructure, as confirmed by the findings. The implementation of Israeli early threat detection technologies significantly enhanced the protection of Ukraine's critical infrastructure, making this case of practical interest for other countries facing similar threats.

Thus, international cooperation in the field of cybersecurity demonstrated a positive development dynamic, particularly in multilateral formats. The identified trends indicated the formation of a new paradigm of international security, in which cybersecurity played a key role. At the same time, challenges remained concerning the harmonisation of national legislation, particularly in the area of procedural investigation mechanisms and the collection of digital evidence. Further development of international cooperation required a comprehensive approach that combined legal, institutional, and technological aspects of combating cybercrime while taking into account the need to protect fundamental human rights.

Conclusions

The study confirmed the transformation of cybersecurity from a purely technological tool into an intergovernmental instrument of geopolitical-level interaction. In cyberspace, traditional state borders lost the effectiveness, and countering cyber threats required coordination at the level of international actors. The transnational nature of cybercrime necessitated the development of adaptive international legal mechanisms, as individual efforts by separate states did not provide an adequate level of protection for the information space. An analysis of international legal mechanisms for combating cybercrime showed the evolution and gradual improvement in effectiveness. The Budapest Convention established standards for combating cybercrime. The elaboration of mechanisms was carried out through regional instruments and the creation of specialised institutions, which contributed to improved results in international cooperation.

A comparative analysis of international legal mechanisms revealed greater effectiveness of legal assistance within EU instruments, which was attributed to detailed regulation of cooperation procedures and the existence of effective mechanisms for monitoring the fulfilment of obligations. The analysis of the implementation of these mechanisms in national legislations confirmed a differentiated level of success: the legal definition of cybercrime offences was implemented in 45 countries, mechanisms of international cooperation in 42 countries. At the same time, only 38 countries implemented procedural norms for investigations, and the collection of digital evidence was fully reflected in the legislation of only 35 countries, which indicated the need for further harmonisation in these areas.

Case analysis of international cooperation in the field of cybersecurity demonstrated the effectiveness of multilateral formats. The Polish-NATO format enabled the reduction of response time to cyber incidents from 24 to 4 hours due to the operation of a network of 24/7 response points. Within NATO, a trust fund contributed to a 47% increase in the effectiveness of responses to attacks following the establishment of a situational centre. As part of Ukrainian-Israeli cooperation, the frequency of successful attacks on critical infrastructure decreased by 39%, while the US-Ukrainian format, formalised through the Ukraine Cybersecurity Cooperation Act, ensured comprehensive support for Ukraine's cyber systems.

Four factors were identified as determining the effectiveness of international cooperation in the field of cybersecurity: the existence of a clear legal basis, stable coordination mechanisms, technological compatibility of protection systems, and regular exchange of threat information. Multilateral formats of cooperation, such

as NATO and EU mechanisms, provided access to more effective expert and technical potential, making these formats the most efficient. Going forward, it is advisable to analyse cooperation mechanisms in more detail, develop preventive strategies to counter cybercrime, and create unified models of global cyber protection that take into account human rights, rapid response, and legal standards.

Acknowledgements

None.

Funding

The research received no funding.

Conflict of Interest

None.

References

[1] Agreement between Ukraine and the European Police Office on operational and strategic cooperation. (2023, February). Retrieved from https://zakon.rada.gov.ua/laws/show/984_001-16#Text.

[2] Agreement on the Implementation of the NATO-Ukraine Cybersecurity Trust Fund between the Security Service of Ukraine and the Romanian Information Service. (2015, July). Retrieved from https://zakon.rada.gov.ua/laws/show/642_063#Text.

[3] Albakjaji, M., & Almarzoqi, R. (2023). The impact of digital technology on international relations: The case of the war between Russia and Ukraine. *Access to Justice in Eastern Europe*, 8.

[4] Biedron, S.R. (2024). *Cybercrime in the digital age.* (Master Thesis, University of Oxford, Oxford, Great Britain). doi: 10.5287/ora-r8oxybrng.

[5] Broeders, D., Cristiano, F., & Weggemans, D. (2023). Too close for comfort: Cyber terrorism and information security across national policies and international diplomacy. *Studies in Conflict & Terrorism*, 46(12), 2426-2453. doi: 10.1080/1057610X.2021.1928887.

[6] Buçaj, E., & Idrizaj, K. (2025). The need for cybercrime regulation on a global scale by the international law and cyber convention. *Multidisciplinary Reviews*, 8(1), article number e2025024. doi: 10.31893/multirev.2025024.

[7] Campina, A., & Rodrigues, C. (2022). Cybercrime and the council of Europe Budapest convention: Prevention, criminalization, and international cooperation. In *The book of full papers – 7th international zeugma conference on scientific researches* (pp. 112-123). Ankara: IKSAD.

[8] Cherniavskyi, S., Babanina, V., Mykytchyk, O., & Mostepaniuk, L. (2021). Measures to combat cybercrime: Analysis of international and Ukrainian experience. *Cuestiones Políticas*, 39(69). doi: 10.46398/cuestpol.3969.06.

[9] Clough, J. (2023). Lessons in a time of pestilence: The relevance of international cybercrime conventions to controlling post-pandemic cybercrime. In *Cybercrime in the pandemic digital age and beyond* (pp. 131-151). Cham: Springer International Publishing. doi: 10.1007/978-3-031-29107-4_7.

[10] Çomak, H., Şeker, B.Ş., Civelek, Y., & Bozkuş, Ç.A. (Eds.). (2022). *Cyber environment and international politics*. London: Transnational Press.

[11] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. (1981, January). Retrieved from https://rm.coe.int/16808ade9d.

[12] Convention on Cybercrime. (2001, November). Retrieved from https://rm.coe.int/1680081561.

[13] Cybersecurity Ventures. (2023). *Cybercrime to cost the world $9.5 trillion annually by 2024*. Retrieved from https://cybersecurityventures.com/cybercrime-to-cost-the-world-9-trillion-annually-in-2024/.

[14] Directive of the European Parliament and of the Council No. 2013/40/EU "On Attacks Against Information Systems and Replacing Council Framework Decision No. 2005/222/JHA". (2013, August). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32013L0040.

[15] Dumchykov, M., Utkina, M., & Bondarenko, O. (2022). Cybercrime as a threat to the national security of the Baltic States and Ukraine: The comparative analysis. *International Journal of Safety and Security Engineering*, 12(4), 481-490. doi: 10.18280/ijsse.120409.

[16] EU Regulation on the European Cybercrime Centre (EC3). (2013). Retrieved from https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3.

[17] Gajjar, V.R., & Taherdoost, H. (2024). Cybercrime on a global scale: Trends, policies, and cybersecurity strategies. In *2024 5th International conference on mobile computing and sustainable informatics (ICMCSI)* (pp. 668-676). Lalitpur: IEEE. doi: 10.1109/ICMCSI61536.2024.00105.

[18] Geneva Declaration of Principles. (2003, February). Retrieved from https://zakon.rada.gov.ua/laws/show/995_c57#Text.

[19] Graham, A. (2023). *Cybercrime: Traditional problems and modern solutions*. (Doctoral ddissertation, Victoria University of Wellington, Wellington, New Zealand). doi: 10.26686/wgtn.22300909.

[20] Internet Crime Complaint Center (IC3). (2024). *Internet crime report 2023*. Retrieved from https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf.

[21] Internet Organised Crime Threat Assessment (IOCTA). (n.d). Retrieved from https://www.europol.europa.eu/publications-events/main-reports/iocta-report.

[22] Jiang, S. (2023). A new mechanism of international law for combating cybercrime. *Law Sciences*, 2(181).

[23] Kolomiiets, N., Senchenko, N., Petryk, O., Ivankov, I., Ovsiannikova, O., & Geperidze, D. (2023). International legal standards in crime prevention. *WSEAS Transactions on Environment and Development*, 19, 110-118. doi: 10.37394/232015.2023.19.10.

[24] Law of Ukraine No. 2163-VIII "On the Basic Principles of Cybersecurity of Ukraine". (2018, July). Retrieved from https://zakon.rada.gov.ua/laws/show/2163-19.
[25] Muhammad, I.A. (2023). Assessment of the impact of information technology on Nigeria's international relations. *Social Science Research Network*. doi: 10.2139/ssrn.4483966.
[26] Mujtaba, B.G. (2023). Operational sustainability and digital leadership for cybercrime prevention. *International Journal of Internet and Distributed Systems*, 5(2), 19-40. doi: 10.4236/ijids.2023.52002.
[27] OECD Guidelines on Managing Digital Risks for Economic and Social Prosperity. (2015). Retrieved from https://www.oecd.org/sti/ieconomy/digital-security-risk-management.htm.
[28] Office of Inspector General U.S. Agency for International Development. (2018). *Audit of USAID's financial statements for fiscal years 2018 and 2017*. Retrieved from https://oig.usaid.gov/node/1851.
[29] Opening Remarks by Acting DCM Joseph Pennington at the U.S.-Ukraine Cyber Bilateral Dialogue. (2020). Retrieved from https://ua.usembassy.gov/opening-remarks-by-acting-deputy-chief-of-mission-joseph-pennington-at-the-u-s-ukraine-cyber-bilateral-dialogue/.
[30] Pallangyo, H.J. (2022). Cyber security challenges, its emerging trends on latest information and communication technology and cyber crime in mobile money transaction services. *Tanzania Journal of Engineering and Technology*, 41(2), 189-204. doi: 10.52339/tjet.v41i2.792.
[31] Poe, L. (2021). Cybercrime in the age of digital transformation, rising nationalism and the demise of global governance. In *Modern police leadership: Operational effectiveness at every level* (pp. 109-126). Cham: Palgrave Macmillan. doi: 10.1007/978-3-030-63930-3_11.
[32] PWCyber cooperative programme in cyber security. (2019). Retrieved from https://www.gov.pl/attachment/6b21cff9-d133-4079-b193-170f9648d486.
[33] Rakhimberdieva, O. (2023). The impact of digital technologies on international relations: A structural analysis. *Galaxy International Interdisciplinary Research Journal*, 11(12), 1468-1474.
[34] Resolution of General Assembly No. A/RES/74/247 "On Countering the Use of Information and Communications Technologies for Criminal Purposes". (2019, December). Retrieved from https://undocs.org/A/RES/74/247.
[35] Resolution of the Cabinet of Ministers of Ukraine No. 497 "On Approval of the Agreement on Cooperation of the Member States of the Commonwealth of Independent States in Combating Crime". (2001, March). Retrieved from https://zakon.rada.gov.ua/laws/show/497-99-%D0%BF#Text.
[36] Resolution of the UN Security Council No. 2341 "On the Protection of Critical Infrastructure from Terrorist Attacks". (2017, February). Retrieved from https://undocs.org/S/RES/2341(2017).
[37] Rohmat, A., Putri, H.A.A., Muhtarom, M., Ismiyanto, I., & Febriani, A.F. (2024). Potential cybercrime and prevention in the overseas official travel approval letter. *AL-MANHAJ: Jurnal Hukum dan Pranata Sosial Islam*, 6(1), 87-98. doi: 10.37680/almanhaj.v6i1.4674.
[38] Segura-Serrano, A. (2021). Cybersecurity and cybercrime: Dynamic application versus norm-development. *Journal of Comparative Public Law and International Law/Heidelberg Journal of International Law*, 81(3), 701-732. doi: 10.17104/0044-2348-2021-3-701.
[39] Shakhbazian, K. (2021). Cooperation of states in the field of combating cyber crime and approaches to solving the problem of cyber terrorism. *Actual Problems of International Relations*, 1(148), 35-48. doi: 10.17721/apmv.2021.148.1.35-48.
[40] Shires, J. (2024). Career connections: Transnational expert networks and multilateral cybercrime negotiations. *Contemporary Security Policy*, 45(1), 45-71. doi: 10.1080/13523260.2023.2274775.
[41] Siabro, A. (2021). International law and international relations. *European Political and Legal Discourse*, 8(5), 6-13. doi: 10.46340/eppd.2021.8.5.1.
[42] Siregar, G., & Sinaga, S. (2021). The law globalization in cybercrime prevention. *International Journal of Law Reconstruction*, 5(2), 211-227. doi: 10.26532/ijlr.v5i2.17514.
[43] The Cybersecurity Strategy. (2020, July). Retrieved from https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy.
[44] The IDF Strategy. (2016, July). Retrieved from https://www.inss.org.il/he/wp-content/uploads/sites/2/2017/04/IDF-Strategy.pdf.
[45] The Situation Centre for Cybersecurity was opened. (2018). Retrieved from https://uteka.ua/ua/publication/news-14-delovye-novosti-36-otkryli-situacionnyj-centr-obespecheniya-kiberbezopasnosti.
[46] Ukraine Cybersecurity Cooperation Act. (2017, February). Retrieved from https://www.congress.gov/bill/115th-congress/house-bill/1997/text.
[47] World Economic Forum. (2024). *Global cybersecurity outlook 2024*. Retrieved from https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2024.pdf.
[48] Yemets, O., Voronov, I., & Hribov, M. (2024). Legal aspects of international cooperation in combating organised crime. *Scientific Journal of the National Academy of Internal Affairs*, 29(1), 20-30. doi: 10.56215/naia-herald/1.2024.20.