DOI: https://doi.org/10.57125/FEL.2023.09.25.05

How to cite: Macidov, S. T. oglu (2023). Prosecuting Cybercrimes under International Legal Frameworks: Challenges and Innovations. *Futurity Economics&Law, 3*(3). 80-96. https://doi.org/10.57125/FEL.2023.09.25.05

Prosecuting Cybercrimes under International Legal Frameworks: Challenges and Innovations

Macidov Sayyad Tofiq oglu

PhD in Law, Professor of Justice Academy of Ministry of Justice of Azerbaijan Republic, Assistant Professor of Baku Eurasian University, https://orcid.org/0000-0003-3541-6893

Corresponding author: *sayyad.macid@mail.ru.*

Received: May 2, 2023 | **Accepted:** August 13, 2023 | **Published:** September 25, 2023

Abstract: Combating cybercrime is one of the most relevant areas of legal community development since the widespread integration of digital technologies into all human activity demonstrates the need to regulate this sensitive area. The aim is to study the international legal framework for countering cybercrime and the system of challenges and innovations that exist in the modern world. The research method used was a systematic review conducted through the LexisNexis, Westlaw, Scopus, and Web of Science databases among publications from 2010 to 2023. As a result of applying inclusion and exclusion criteria, 56 relevant studies were identified, and their texts were subjected to content analysis. In the article, modern interpretations of the term "cybercrime" were defined, and certain legal international agreements that counteract its spread (primarily the Budapest Convention as an essential current document of modern legal influence) and trace the mechanisms of counteraction and methods of their improvement were examined. Other critical legal acts, such as the European Union Directive on the prevention of cyber-attacks on information systems and the European Commission Directive on combating fraud and other financial crimes on the Internet, were also considered. As a result, it was found that there were differences at the interstate level in the organisation of the cooperation, which included multilateral and bilateral agreements. The identified problems included insufficient interaction between the law enforcement agencies of different countries at the relevant stages and the lack of an agreed mechanism for obtaining external data. The conclusions established that close ties at the level of international law enforcement systems aimed at addressing cybercrime issues could effectively overcome these difficulties.

Keywords: cybercrime, international law, conventions, counteraction, challenges.

Introduction

In today's world, flooded with advanced technologies and a deeply integrated Internet network, the concept of borderless crime is taking on new and more complex shades. The cyberspace, once a symbol of communication and knowledge, has now become an arena for the development of dangerous cybercrime that can instantly turn digital progress into a challenge to security and stability. The growth of cyberattacks, from identity theft to cyberespionage and cyberterrorism, requires a deep understanding and effective response to these threats at the international level.

In this context, the international community is actively working in order to establish a legal framework that will regulate the cybercrime liability and ensure its effective prosecution. However, this process is not an easy task due to the controversial and complex nature of cybercrime itself, which can transcend national borders and cause legal uncertainty. On the one hand, there are traditional legal instruments that can be applied to cybercrime, but on the other hand, the need for adaptation and innovative approaches is becoming more important than ever.

Research Problem

The research problem requires a deep understanding of both the technical aspects of cybercrime and the legal requirements governing their prosecution. It is important identifying the diverse international documents and conventions that regulate the prevention and punishment of cybercrime. A closely related to this issue is the extent to which the global community is ready to work together to confront this challenge without resorting to manipulation or abuse of its position. It is equally important in the current context of the integration of digital technologies into public life to identify the types of cybercrime and the possible consequences of their spread. The tools of legal uncertainty in considering and proving the guilt of cybercrime suspects, as well as the introduction of innovative tools to combat the cybercrime, are relevant for study, so that the international community can prevent their organisation or at least reduce the consequences.

Research Focus

Therefore, this article offers an in-depth analysis of the challenges faced by regulation enforcement agencies and international legal structures in prosecuting the cybercrime, focusing on the international legal framework and the need for innovative approaches to effectively address this new wave of crime. Ways of cooperation between countries, the development of new technologies, and even redefining cybersecurity all play a role in creating a sustainable and effective international approach to the cybercrime.

Research Aim and Research Questions

The aim of the study is to examine the international legal framework, challenges and innovations which are provided for the prosecution of the cybercrime. To achieve the purpose of the article, the following problematic issues were considered:

1. To define the essence of the term “cybercrime”.

2. To analyse the fundamental international instruments governing the fight against digital crime.

3. To describe the difficulties that exist in the implementation of countering the cybercrime in the international legal field

Research hypotheses proposed in the article:

1. The cybercrimes in international documents need to be specified and can lead to abuses in countries with authoritarian or totalitarian regimes (based on the consideration of the future UN treaty on security in the digital sphere)

2. The correlation between the effectiveness and ineffectiveness of international treaties and norms of national legislation, based on a thorough review of the main international legal documents.

Literature Review

Some aspects of the digital relations development and the problems of implementing mechanisms to counter the cybercrime have been considered by modern scholars. Particularly, Alsemairi (2022) described the importance of digital technologies in combating human trafficking crimes on the Internet. According to these authors digital technologies play a crucial role in combating human trafficking crimes on the internet. Human trafficking is a global criminal enterprise that has evolved alongside technological advancements, and law enforcement agencies and organisations dedicated to fighting this heinous crime have leveraged digital tools to enhance their efforts. Boiko (2020) and Boiko (2021) describe the key aspects of legal regulation of combating various types of crimes. Thus, the legal regulation of combating various types of crime is a multifaceted and complex field that involves numerous aspects of law enforcement, criminal justice, and public policy. Other authors also addressed this problem (See Table 1).

Table 1

Key aspects of legal regulation

Criminal Legislation	Laws and statutes define specific crimes, their elements, and penalties. Legislators create and amend these laws to address emerging criminal activities (Marzano, 2022; Radu & Rook, 2022).
Law Enforcement	Police agencies investigate crimes, gather evidence, and apprehend suspects. Coordination between local, state, and federal law enforcement agencies is crucial to effectively combatting crime (Chirita, 2021; Boiko, 2021).
Prosecution	District attorneys and prosecutors bring charges against individuals accused of committing crimes. Prosecutors must prove guilt beyond a reasonable doubt during criminal trials (Gangwar & Narang, 2022; Boiko, 2021).
Criminal Justice System	Courts adjudicate criminal cases and ensure due process. Judges and juries decide guilt or innocence and impose sentences when necessary (Marzano, 2022; Radu & Rook, 2022).
Rehabilitation and Corrections	Prisons and correctional facilities are used to house and rehabilitate convicted individuals (Yeboah-Ofori & Opoku-Boateng, 2023.) Rehabilitation programs aim to reduce recidivism and reintegrate offenders into society (Boiko, 2020).
Prevention	Crime prevention initiatives involve public education, community policing, and outreach programs (Peresada, 2021; Boiko 2021). Targeted

	interventions aim to address the root causes of criminal behavior (Zabarniy et al., 2022).

Source: compiled by the authors

According to Dilek et al. (2015), the level of impact of cybercrime is bigger compared to another crimes, as it is felt at the, national, personal, societal and transnational levels. According to Cardoza & Wagh (2017), developing countries are at greater risk from this type of crime. Therefore, these scholars believe that the fight against the cybercrime requires a strategic and intelligent system. At the same time, the current scientific literature also describes in detail the composition of the cybercrime and its key features (Turrini & Ghosh, 2010) (see Table 2).

Table 2

The main signs of cybercrime

Feature	Explanation
Subject of the offence	The subjects of the cybercrime are physical sane individuals who have reached the age of sixteen at the time of the crime.
Subjective side	It is defined by direct intent and, as a rule, a mercenary motive
Object of the crime	The social relations on which cybercriminals rely
The objective side	This feature is determined by several components: 1. A socially dangerous act 2. Socially dangerous outcome 3. Causal statements between actions and outcomes 4. Place, instrument, method and means of committing the offence

Source: compiled by the authors

The study by Kurebwa & Magumise (2020) notes that in the investigation of the cybercrime, considerable attention should be paid to supporting victims in updating damaged or lost information. At the same time, the current literature notes that several modern approaches to combating the cybercrime have been used in different regions of the world. In particular, in 2002, the Commonwealth of Nations developed the so-called model law on computer and computer-related crimes, which aims to improve the legislative framework of the Commonwealth member states in the field of combating the cybercrime and improve cross-border cooperation (Malanchuk & Kyrychenko, 2021). In the absence of such a treaty, in order to form international cooperation in this area, the members of the society should conclude a number of bilateral agreements with each other, which would greatly complicate the procedure for implementing cooperation. The Model Law contains, for example, a number of provisions on the specifics of organising international cooperation. The EU member states have made efforts to harmonise the main legislative aspects of cybercrime in force in their territories. For example, Directive 2000/31 of the European Parliament and of the Council on definite legal aspects of the information and electronic community, in particular, on digital commerce in internal market, was adopted (Mohapatra,

2022). At the same time, the framework decision of the Council of the European Union on combating fraud and falsification of non-cash means, etc. is also important.

Nawang (2017) also describes other key legislative frameworks for regulating crimes that use digital and information and communication technologies. So, in addition to the traditional criminal legislation and enforcement mechanisms, there are key legislative frameworks and approaches that are often used to regulate and combat various types of crimes. These frameworks may focus on specific areas of criminal activity or involve specialised agencies and regulations: antitrust and competition laws, environmental laws, intellectual property laws, etc. Rajput (2020) describes the theoretical basis for regulating digital economic crimes. According to this author the theoretical basis for regulating digital economic crimes, such as cybercrimes related to fraud, hacking, and online theft, is rooted in several key principles and concepts. These principles help guide the development of legal and regulatory frameworks aimed at addressing the challenges posed by criminal activities in the digital economy. At the same time, Thomas (2023) outlined the main preventive measures to combat the cybercrime. Preventing cybercrime is a multifaceted effort that involves individuals, organisations, and governments working together to enhance cybersecurity. Some of the main preventive measures to combat cybercrime include: user awareness and education, strong authentication and access control, regular software updates and patch management, intrusion detection systems, etc. However, the need for further scientific research is argued by the existence of certain challenges in modern international law.

Research Methodology

Search Strategy

The systematic review used various academic databases, including LexisNexis, Westlaw, Scopus, and Web of Science, as well as specialised international legal resources such as the United Nations Treaty Collection and the Council of Europe Treaty Office. The primary keywords used in the search query included “cybercrime prosecution,” “international legal frameworks,” “international cybercrime law,” “cross-border cybercrime,” “cybercrime conventions,” and other terms related to international law and cybercrime.

The search was limited to the period from 2010 to 2023 to capture recent developments and international initiatives in the fight against cybercrime.

Inclusion and Exclusion Criteria

The review included articles and legal documents that met the following criteria:

- Thematic relevance (studies and documents related to the international prosecution of cybercrimes);
- Publications in English;
- Full-text documents available;
- Sources published in peer-reviewed journals, international legal bodies, or institutions with official status.

The following publications were excluded:

- Those focused solely on national legal systems without analysis of international aspects;
- Documents available only as abstracts or brief overviews;
- Publications before 2010, unless they contained significant fundamental data for international legal practice.

Screening Process

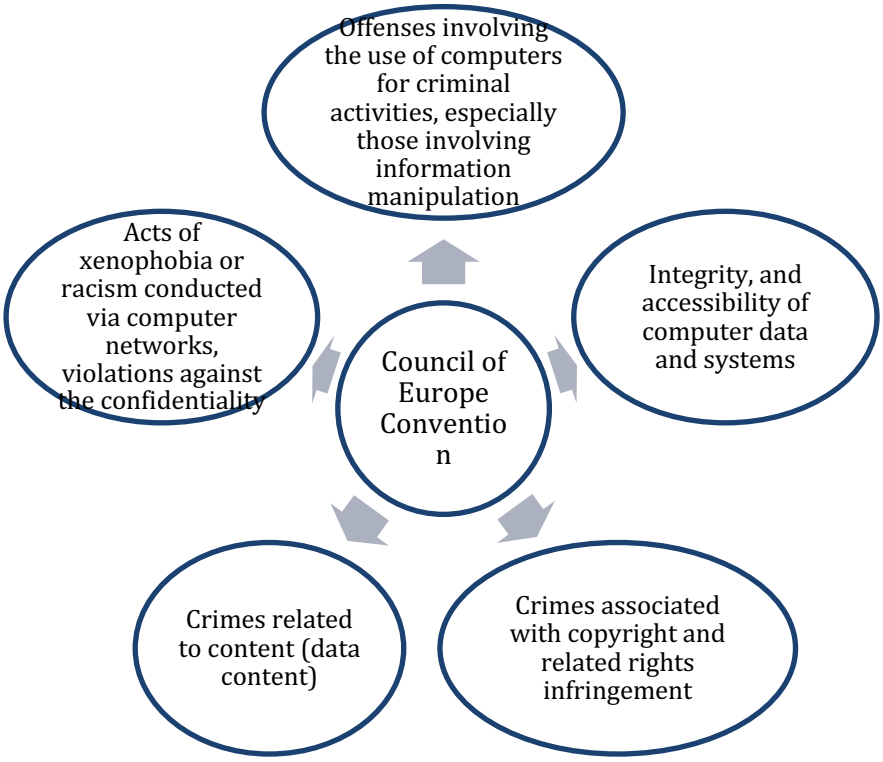
Initially, approximately 454 sources were found. After the preliminary screening (based on titles and abstracts), 221 articles that did not meet the inclusion criteria were excluded. In the second stage, after a detailed full-text analysis, another 177 sources were excluded due to not meeting the strict requirements for international relevance or being outdated in terms of modern legal practice. As a result, 56 relevant sources were selected for final analysis and inclusion in the review.

Research Results

The term "cybercrime" first appeared in American and later European literature in the early 1960s and was interpreted as a failure to observe or violate the rights of others in relation to digital information processing systems. Thus, the cybercrime is a concept that includes computer crime (where a computer is an instrument of crime and information security is the object of crime) and other cases where a computer is a tool or method of crime against property, security, copyright, morality, ethical considerations, etc. Currently, the most common classification of cybercrime is based on the Council of Europe Convention on Cybercrime (2001). This document divides the cybercrime into five distinctive groups (see Figure 1).

Figure 1

Types of cybercrime



Source: Convention on Cybercrime (2002)

Thus, cybercrime is a criminal act committed in cyberspace with the help of computers, networks and technologies. Their main features are complex and include a number of important aspects (see Table 3).

Table 3

The main features of cybercrime

Features	Explanation
Technicality	The cybercrime requires the use of technical knowledge and skills in the field of computers, programming, networks and other technologies.
Remoteness, in some cases anonymity	Criminals can commit cybercrime from a great distance using anonymous tools and networks. This makes it difficult to identify and prosecute criminals.
Diversity of species	The cybercrime covers a wide range of activities, such as hacking, phishing, viruses, identity theft, computer fraud, malware, etc.
Global in nature	The cybercrime can result in serious material, financial and moral damage to the affected individuals, companies, organisations and even states (Deirmenjian, 2000). Criminals can commit cybercrime anywhere in the world, making it a global phenomenon. Cybercrime can become a threat to national security and international cooperation.
Speed and scale	Criminals can commit cybercrime quickly and on a large scale. In particular, viruses and other types of malwares can spread around the world in a matter of hours.
Innovation and constant change	Criminals are constantly looking for new ways to commit cybercrime and circumvent defences. This requires continuous improvement of cybersecurity measures.

Source: compiled by the authors

So, as the modern technology is constantly evolving, the cybercrime is also evolving, making it important to maintain and improve cybersecurity to protect against these threats. At the same time, the Global Cyber Security Index (2020) report suggests that most countries in the world are not yet ready to counter cyber threats. The GCI classifies and divides countries according to their level of cybersecurity. It divides countries into the following categories:

1. The leading stage: countries characterised by high readiness to withstand cyber attacks

2. Developmental stage: countries that are increasingly digitised but still developing the cybersecurity

3. Initial stage: economies are beginning to be digitised (Chirita, 2021).

The current report indicates that only more than 20 countries are in the advanced stage, and 96 countries are still in the early stages (see Table 4 and Figure 1). In Figure 2 described the ranking of the 10 most significant countries in the digital transformation system.

Table 4

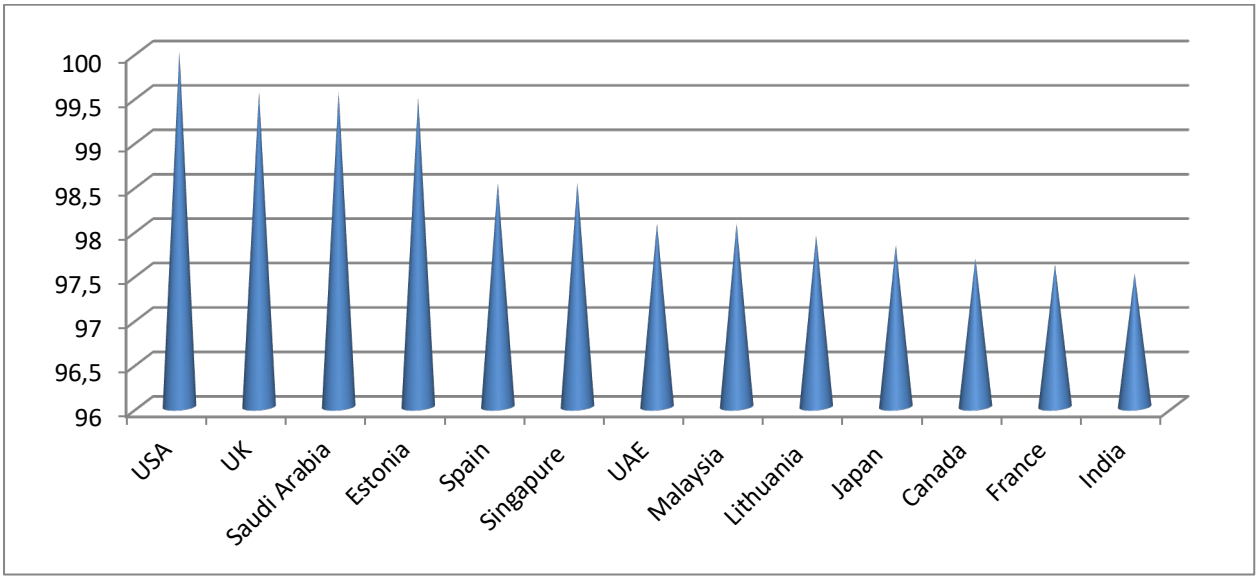
Country rankings based on the Global Cyber Security Index

Country	Assessment	Rank
United States of America	100	1
United Kingdom	99. 54	2
Saudi Arabia	99. 54	2
Estonia	99. 48	3
Singapore	98. 52	4
Spain	98. 52	4
United Arab Emirates	98. 06	5
Malaysia	98. 06	5
Lithuania	97. 93	6
Japan	97. 82	7
Canada	97. 67	8
France	97. 6	9
India	97. 5	10
Germany	97. 41	13
Greece	93. 98	23
Poland	93. 86	30
Georgia	81. 06	55
Ukraine	65. 93	78

Source: Global Cyber Security Index (2020)

Figure 2

The ranking of the 10 most significant countries in the cyber transformation system

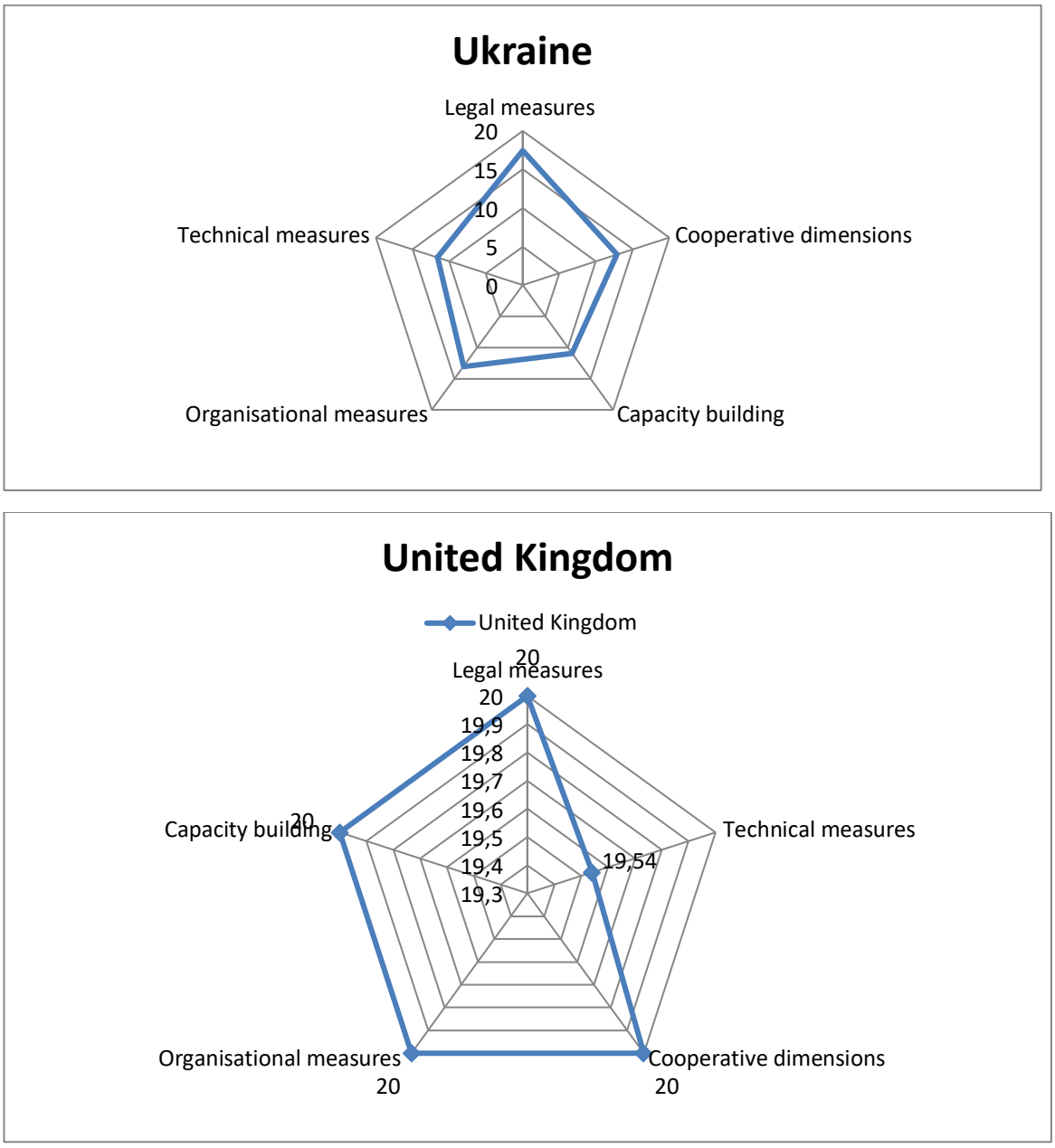


Source: Global Cyber Security Index (2020)

This report identifies that Ukraine's area of relative strength is in legal measures. At the lowest level are capacity building, cooperative and technical measures. For comparison, the UK system (99.54) is ranked as having relative strength in legal, organisational, and cooperative aspects of development (see Figure 3-4).

Figure 3-4

Indicators of cyber development in Ukraine and the UK



Source: Global Cyber Security Index (2020).

Therefore, given the UK's high performance in the field of legal measures, technical dimensions that generally affect the country's cyber environment play an important role in improving. Therefore, an important approach to implementing the fight against the cybercrime in the international context of cross-border cooperation is the creation and standardisation of a modern legal framework.

The Budapest Convention on Cybercrime, adopted in 2001, is one of the main international documents designed to serve as a basis for combating the cybercrime at the international level. This international legal instrument is aimed at countering the threatening scale of the cybercrime, ensuring

compliance with the rules and opportunities for ensuring cybersecurity. Although this document was adopted a long time ago, for European countries and all other signatories, the implementation of its provisions has become an important step towards ensuring the security of the digital environment. When analysing the key aspects and essence of this Convention, it is worth emphasising the objectives and object of the international document. The main goal of the Budapest Convention is to establish a unified international legal framework for combating cybercrime (Convention on Cybercrime, 2002). The document was created to facilitate cooperation between countries in the detection, prosecution and punishment of the cybercrime offenders, as well as to ensure effective legal protection against such crimes. Certain provisions of the Convention establish a classification of crimes, defining a fairly wide range of such offences. In particular, the Convention defines such types of cybercrime as data misuse, computer fraud, copyright infringement, network security breaches, activities that facilitate network security breaches and other similar crimes.

The adoption of the Convention was an open attempt to establish cooperation between countries in this sensitive area. The Convention enables countries to cooperate in the detection, collection of evidence and prosecution of cyber criminals. It provides for the exchange of information, assistance in investigations and execution of extradition requests (Convention on Cybercrime, 2002). The document also addresses the issue of human rights protection, which has received considerable attention in the context of combating offences in the digital world. The Convention recognises the need to ensure privacy, freedom of expression and other rights in cyberspace.

In order to enhance cooperation, the document also provides for the establishment by the parties at the national level of a body to maintain permanent contacts for the purpose of providing urgent assistance in the prosecution of the cybercrime. Such assistance includes the facilitation or, where permitted by national law, the unconditional provision of technical advice (see Table 4).

Table 4

The legal framework for the provision of urgent assistance in the prosecution of cybercrime (based on the Budapest Convention)

Principle.	Articles
A) providing technical advice	Articles: 25, 31, 33
B) Keeping important information safe	Article 29, 30
C) Collecting evidence, providing legal information and locating suspects	Article 35

Source: Convention on Cybercrime (2002)

The Additional Protocol to the Convention, adopted in 2006, criminalised the dissemination of racist and xenophobic acts on the Internet. Accordingly, any manifestations of these negative phenomena, insults or threats based on racism or xenophobia are prosecuted at the international level. In order to respond to the challenges, it is proposed to ensure the existence of an effective system of law enforcement in the field of combating cybercrime. However, the primary focus is not on the formation of separate supranational law enforcement structures, but only on establishing a fast and reliable exchange of information and evidence between countries about identified threats (Marzano, 2022).

At the same time, the Convention serves only as a certain advisory document against the background of national legislation of the signatory countries. The Convention allows countries making a reserve in the interpretation and implementation of certain provisions that may contradict their national legislation or constitutional principles (Shipley & Bowker, 2014). Unfortunately, this provision opens up a wide range of possible abuses of the Convention and, to some extent, undermines its value

as an international legal instrument. The Convention and the Explanatory Report were adopted at the 109th session of the Committee of Ministers of the Council of Europe in November 2001 and finally signed in Budapest the same month, but the Convention entered into force in July 2004, which allowed signatory countries to adapt their national legislation to the international document (Cardoza & Wagh, 2017).

Thus, as of April 2023, 63 countries have ratified the Budapest Convention, and several more have officially signed it, but national parliaments have refused to ratify it. India exercised its right not to ratify the Convention (officially because the country did not participate in its development). However, because of the outbreak of cybercrime, the government of this Asian state is ready to reconsider this option. The Kremlin regime has also not signed the Budapest Convention, which can be explained by its aggressive policy towards its neighbours and in the international arena in general. In addition, the official Kremlin publicly uses elements of racism and xenophobia in its activities, with some success in spreading such topics in the Russian digital world "for internal use." The fact that the Convention was not approved by the Chinese government also made it vulnerable. As a result, one of the largest modern digital powers has abandoned the restrictive document and unleashed its own hands in the interpretation and conduct of cybersecurity.

To summarise, the Budapest Convention is an important step in creating an international legal mechanism to combat the cybercrime. It creates a framework for cooperation between countries, which is an important aspect in the globalised digital space. However, given the rapid changes in technology and the nature of cybercrime, it is important to constantly update and adapt this legal instrument to meet new challenges and innovations in cybersecurity.

The European Union is implementing a set of measures envisaged by regulatory and legal acts aimed at combating illegal actions aimed at violating electronic information resources. Such acts include the EU Directive on countering cyber-attacks on information systems, adopted in 2013, and the European Commission Directive on combating fraud and other financial crimes on the Internet, adopted in 2017.

The European Union pays considerable attention to early detection and rapid response to cyber incidents and cyber-attacks against electronic information resources. For example, the European Network and Information Security Agency plays a significant position in ensuring the detection and blocking of cyber-attacks, as well as the localisation of their consequences, regardless of their origin, and this applies to civilian objects of all forms of ownership. Additionally, an entity called CERT-EU (Computer Emergency Response Team) detects cyberattacks by using a specialised technological system of sensors located on subscriber access lines to servers (Franjić, 2023). When a sensor is triggered, CERT-EU is immediately notified of a cyberattack. If CERT-EU detects signs of criminal activity, the relevant information is sent to the European Cybercrime Centre (ECC), which in turn can notify the European Defence Agency (EDA) to organise cyber operations or the European External Action Service (EEAS) (Kurebwa, & Magumise, 2020). In line with the goal of creating an enabling environment for the progress of digital technologies, the UN's New Partnership for Africa's Development programme is working with the African Union Commission to develop a convention on cybersecurity in Africa.

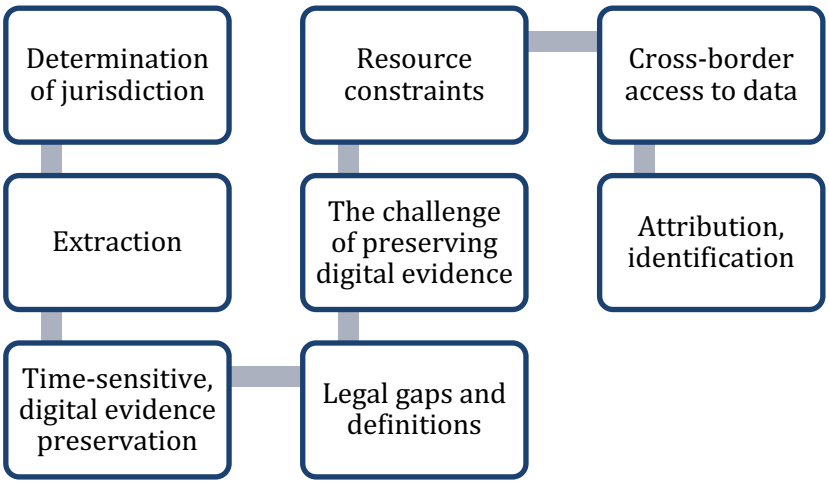
At the international level, there are discrepancies in the issues of cooperation included in bilateral documents. There is also a lack of obligation to provide responses within a set timeframe, as well as a lack of agreed direct access to extraterritorial data. The many informal networks of law enforcement agencies and differences in the guarantees of cooperation lead to serious problems in achieving successful global assistance on digital evidence in different criminal cases. In addition, the concept of the UN Convention on International Information Security was developed, where Article 4 sets out the

main threats to global harmony and safety in the information space (Marzano, 2022). In particular, 11 basic and 4 additional threats are specified, including the use of information technologies for hostile acts and acts of aggression, destructive impact on critical structures and cross-border dissemination of information that violates international law and national legislation.

In summary, the prosecution of cybercrime under the international legal framework presents several important challenges stemming from the evolution of technology and the complexities of cross-border jurisdiction. These challenges often impede effective law enforcement and cooperation between countries in combating the activities of cybercriminals. Figure 5 summarises the key challenges to the effective prosecution of cybercrime based on an analysis of international legal instruments.

Figure 5

Key challenges to the effective organisation of cybercrime prosecution



Source: compiled by the authors

Given the outlined above challenges, it should be noted that determining jurisdiction in cybercrime cases can be difficult due to the borderless of the Internet. Cybercriminals may operate from one country while targeting victims in another, making it difficult to determine which country's laws apply and where prosecutions should take place. In the process of prosecuting the cybercrime, an important issue is the identification of the true identity and location of cybercriminals. Attackers can use techniques to hide their tracks, such as routing attacks through multiple servers, using anonymisation tools, and using compromised systems. This makes it difficult to attribute the cybercrime to specific individuals or groups (Garasim, 2023). At the same time, extraditing cybercriminals to face justice in another country can be difficult due to legal, political and diplomatic barriers. Some countries may not have the appropriate laws to prosecute cybercrime, or they may not consider cybercrime to be an extraditable offence. In addition, some countries may lack the resources, technology and expertise necessary to effectively investigate and prosecute the cybercrime. This may lead to differences in enforcement capabilities in different jurisdictions. The speed at which the cybercrime occurs and the potential for data loss require a rapid response. In some situations, traditional legal procedures for obtaining evidence can be time-consuming, which prevents the timely collection of important information. In addition, it should be recognised that the rapid development of technology often outpaces the development of comprehensive cybercrime laws. Definitions of the cybercrime and legal frameworks may differ from country to country, making harmonisation and cooperation difficult. Ultimately, ensuring the integrity of digital evidence is crucial in cybercrime prosecutions. However, preserving electronic evidence while maintaining a chain of custody can be challenging, which can lead to admissibility issues in court.

Addressing these challenges requires international cooperation, harmonisation of legislation and the development of frameworks that facilitate a cross-border cooperation. Organisations for example, Interpol, Europol and the United Nations Office on Drugs and Crime play an important role in facilitating international cooperation and building capacity to effectively combat the cybercrime.

Discussion

The key problems of solving the "cross-border" cybercrime also include the territorial separation of the traces of the crime and their storage for a limited period of time (DeAngelis, 2000).

In some cases, it is difficult for law enforcement to identify the main areas where this type of crime is committed (Feeley, 2019). Cybercriminals have a high level of anonymity, and the information stored in computers is short-term in nature (Carabellese et al., 2014). At the same time, contemporary scholars agree that the effectiveness of prosecuting cybercrime under the international legal framework depends on cooperation, harmonisation of laws, closing gaps in legislation, technological progress and ongoing dialogue between countries (Gangwar & Narang, 2022; Rajput, 2020). As the digital landscape evolves, international efforts continue to adapt to new challenges in combating cybercrime while adhering to the principles of fairness and accountability (Marzano, 2022).

The analysed Budapest Convention and other documents are important international treaties on crimes committed via the Internet, digital communication networks and cyberspace (Gronowska, 2019). The 2001 Convention and its supplementary protocols contain normative provisions that regulate such crimes as copyright infringement, computer fraud, distribution of child pornography, security network violations, unauthorised access to closed computer systems or databases, fraud or forgery, and countering illegal interception of data. A vulnerability of the Convention as a legal act is that it is signed by a limited number of states. For this reason, researchers are discussing the issue of a single UN treaty on cybercrime, which would be binding on all 193 member states (Malanchuk & Kyrychenko, 2021). The Ad Hoc Committee was entrusted with the development of this Treaty. According to the published materials, it will deal with the organisation of international cooperation, particularly in the area of providing law enforcement agencies with access to potential digital evidence. And although the main content of the Treaty will be based on the existing Budapest Convention on Cybercrime, some organisations and researchers working on the protection of digital rights note problems in implementing the Treaty in an accessible form (Yeboah-(Ofori & Opoku-Boateng, 2023).

For example, researchers also note that the wording of the cybercrime proposed in the future UN Treaty is too broad and does not mention the existence of a mandatory motive for a digital security breach (Karska & Karski, 2019; Kurebwa & Magumise, 2020). In other words, the effect of international law can be turned against anyone who has taken certain actions in the digital space that others do not like. Probably the first at risk are independent researchers, journalists, and hacker groups that do not intend to harm others. A novelty of the UN Treaty is the prosecution of crimes such as the dissemination of false information that could lead to the organisation and conduct of social unrest (Mohapatra, 2022). It is also proposed to prosecute calls for subversive or armed activities in the digital dimension. In practice, many authoritarian states take advantage of the ambiguity in the definition of such concepts as terrorism, riots, etc. to introduce politically motivated arrests and prosecutions (Alnakeep, 2022). For this reason, one should agree with researchers that working with specific definitions in the international legal framework governing cybercrime will require further analysis (Gangwar & Narang, 2022; Mohapatra, 2022). At the present stage, unlawful actions against individuals or organisations are possible under the guise of combating the cybercrime at the international level. Based on this, specific definitions should be given special attention.

The opinions of researchers concerning the correlation between national legislation and international law in the field of ensuring order in cyberspace are also relevant (Rajput, 2020; Zahoor &

Razi, 2020). First of all, it should be said that, due to certain circumstances, authoritarian regimes are able to abuse the right to prosecute. Obviously, the next international legal acts in the field of combating the cybercrime should take this aspect into account and, at the legislative level, cut off the possibilities for abuse of state authorities, violation of citizens' rights, etc.

Conclusions and Implications

Therefore, in the modern legal sense, the cybercrime is understood as a specific concept that primarily refers to the computer crime, where the main instrument of a crime against an information system is a computer or other modern gadget and other cases where a computer is the main tool or method of criminal action against property, security or copyright, ethical considerations, etc. Their main characteristics are darkness, remoteness and anonymity, diversity of types, globalisation, speed and innovation. At the international level, one of the fundamental documents is the Budapest Convention of 2001, which has been ratified by 63 states. The number of states that have agreed to implement its provisions is the document's most vulnerable point. Some countries (including authoritarian or semi-authoritarian regimes in the Kremlin or Beijing) have not accepted the functioning of the Convention. Important legal acts regulating the fight against cybercrime are the EU Directive on countering cyberattacks on information systems, adopted in 2013, and the European Commission Directive on combating fraud and other financial crimes on the Internet, adopted in 2017. An analysis of these documents has shown that there are differences at the interstate level in the organisation of cooperation included in multilateral and bilateral agreements. Among the problems are the lack of timely interaction between law enforcement regimes of different countries and the absence of an agreed possibility of direct access to extraterritorial data. Many bureaucratic obstacles in the cooperation of law enforcement agencies from different countries lead to serious problems in achieving effective international cooperation on electronic evidence in criminal cases.

In order to overcome these difficulties, it was proposed to establish a cooperation at the level of international law enforcement systems, whose activities are clearly aimed at overcoming the problems of cybercrime. At the same time, the introduction of a single UN treaty on combating digital space crimes is quite problematic due to vague interpretations of the basic concepts, which allows authoritarian regimes to use this tool at the global level to protect their dominant position.

Suggestion for Future Research

Cybercrimes become a pervasive global threat, transcending borders and posing significant challenges to law enforcement and legal systems worldwide. This review seeks to explore the complexities surrounding the prosecution of cybercrimes within the context of international legal frameworks. Thus, it will be effective to overcome the next questions in the future research. Particularly, in the following studies, the main attention should be focused on the study of the main legal and practical issues related to cross-border data sharing for cybercrime investigations. In this case, it is worth investigating the development of international standards for data sharing while safeguarding privacy and data protection rights. At the same time, a separate area of the future research will be the analysis of the state responsibility. The issue of state responsibility refers to the legal doctrine that holds states accountable for their actions, omissions, or failures to prevent or address certain acts, including cybercrimes, when they occur within their jurisdiction or are attributed to them. Therefore, the concept of state responsibility for cybercrimes needs to be explored, especially when cyberattacks are committed or supported by state actors, and the legal mechanisms available to hold states accountable for cybercrimes committed within their jurisdiction should also be assessed. Research in this area can delve into case studies of cyber incidents with state involvement, analyse the role of international law in holding states accountable, and explore ways to enhance the effectiveness of the state responsibility in addressing cybercrimes. So, by delving into these research directions, scholars can contribute to a

deeper understanding of the complexities and nuances of prosecuting cybercrimes within the framework of international law, ultimately helping to shape more effective and responsive legal mechanisms.

Acknowledgements

None.

Conflict of Interest

None.

Funding

The Author received no funding for this research.

References

Alnakeep, H. T. (2022). Internet crimes to legal regulation. *International journal of health sciences*, 6(57), 48856–48876. https://doi.org/10.53730/ijhs.v6ns7.13683

Alsemairi, S. S. (2022). The Role of Digital Technologies in Combating Cyber-Trafficking in Persons Crimes. *Computer and Information Science*, *16*(1), 49. https://doi.org/10.5539/cis.v16n1p49

Boiko, I. (2020). Pravove rehuliuvannia protydii zlochynam z nezakonnoho obihu ta zastosuvannia vohnepalnoi zbroi: zarubizhnyi dosvid [Legal regulation of combating crimes in illegal circulation and use of firearms: Foreign experience]. *Nauka i pravookhorona [Science and law enforcment]*, *50*(4), 30–39. https://doi.org/10.36486/np.2020.4(50).3 (in Ukrainian)

Boiko, I. (2021). Pravove rehuliuvannia protydii zlochynam z nezakonnoho obihu ta zastosuvannia vohnepalnoi zbroi: zarubizhnyi dosvid [Legal regulation of combating crimes in illegal circulation and use of firearms: Foreign experience]. *Nauka i pravookhorona [Science and law enforcment]*, *51*(1), 181–190. https://doi.org/10.36486/np.2021.1(51).19 (in Ukrainian)

Carabellese, F., Candelli, C., Barbieri, C., & Catanesi, R. (2014). Internet mediated crimes and theoretical approaches. *The Journal of Forensic Psychiatry & Psychology*, *26*(1), 1–10. https://doi.org/10.1080/14789949.2014.981562

Cardoza, C., & Wagh, R. (2017). Text analysis framework for understanding cyber-crimes. *International Journal of advanced and applied sciences*, *4*(10), 58–63. https://doi.org/10.21833/ijaas.2017.010.010

Chirita, V. (2021). International Legal Documents on Preventing and Combating Terrorist Crimes. *Internal Security*, *13*(2), 33–34. https://doi.org/10.5604/01.3001.0015.6560

Convention on Cybercrime update. (2002). *Computer Fraud & Security*, *2002*(4), 4–5. https://doi.org/10.1016/s1361-3723(02)00408-6

Deirmenjian, J. M. (2000). Hate Crimes on the Internet. *Journal of Forensic Sciences*, *45*(5), 14824J. https://doi.org/10.1520/jfs14824j

Dilek, S., Cakır, H., & Aydın, M. (2015). Applications of Artificial Intelligence Techniques to Combating Cyber Crimes: A Review. *International Journal of Artificial Intelligence & Applications*, *6*(1), 21–39. https://doi.org/10.5121/ijaia.2015.6102

Feeley, M. M. (2019). Two Models of the Criminal Justice System: an Organizational Perspective. In *Criminal Courts* (p. 201–220). Routledge. https://doi.org/10.4324/9781351160766-5

Franjić, S. (2023). Internet Crimes Against Children and Minors. *Law and Economy*, *2*(4), 9–15. https://doi.org/10.56397/le.2023.04.02

Gangwar, S., & Narang, V. (2022). A Survey on Emerging Cyber Crimes and Their Impact Worldwide. In *Research Anthology on Combating Cyber-Aggression and Online Negativity* (p. 1583–1595). IGI Global. https://doi.org/10.4018/978-1-6684-5594-4.ch080

Garasim, P. (2023). The role and place of public control in the legal mechanism for the prevention of penitentiary crime in Ukraine. *Scientific Journal of Polonia University*, *55*(6), 145–150. https://doi.org/10.23856/5519

Global Cyber Security Index. (2020). https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E

Gronowska, B. (2019). Judicial Dialogue in the Human Rights Domain. *International Community Law Review*, *21*(5), 400–408. https://doi.org/10.1163/18719732-12341409

Karska, E., & Karski, K. (2019). Judicial Dialogue in Human Rights. *International Community Law Review*, *21*(5), 391–399. https://doi.org/10.1163/18719732-12341408

Koteshwar, M., & Singh, B. B. J. (2019). Survey Report on Cyber Crimes and Cyber Criminals Get Protected from Cyber Crimes Review Paper. *International Journal of Computer Sciences and Engineering*, *7*(12), 99–109. https://doi.org/10.26438/ijcse/v7i12.99109

Kurebwa, J., & Magumise, E. (2020). The Effectiveness of Cyber Security Frameworks in Combating Terrorism in Zimbabwe. *International Journal of Cyber Research and Education*, *2*(1), 1–16. https://doi.org/10.4018/ijcre.2020010101

Malanchuk, T. V., &Kyrychenko, V. S. (2021). Legal Problems In The Field Of Combating Crimes Of International Nature Committed By Organized Criminal Groups. *Actual problems of improving of current legislation of Ukraine*, (55), 100–109. https://doi.org/10.15330/apiclu.55.100-109

Marzano, G. (2022). Setting Anti-Cyberbullying Legal Policies. In *Research Anthology on Combating Cyber-Aggression and Online Negativity* (p. 312–330). IGI Global. https://doi.org/10.4018/978-1-6684-5594-4.ch018

Mohapatra, D. (2022). Cyber Security Legal Framework in India. In *Cross-Industry Applications of Cyber Security Frameworks* (p. 91–111). IGI Global. https://doi.org/10.4018/978-1-6684-3448-2.ch005

Nawang, N. I. (2017). Combating anonymous offenders in the cyberspace: An overview of the legal approach in Malaysia. In *2017 2nd International Conference on Anti-Cyber Crimes (ICACC)*. (p. 13–18). IEEE. https://doi.org/10.1109/anti-cybercrime.2017.7905255

Peresada, O. (2021). Qualification of crimes against life: Comparative legal analysis. *Ukrainian Polyceistics: Theory, Legislation, Practice*, *1*(1), 61–67. https://doi.org/10.32366/2709-9261-2021-1-1-61-67

Radu, M. B., & Rook, A. L. (2022). How Theoretical Frameworks Inform the Understanding of the Relationship Between Gender and Cyberbullying. In *Research Anthology on Combating Cyber-Aggression and Online Negativity* (p. 231–242). IGI Global. https://doi.org/10.4018/978-1-6684-5594-4.ch014

Rajput, B. (2020). Legal Framework for Cyber Economic Crimes: A Review. In *Cyber Economic Crime in India* (p. 145–169). Springer International Publishing. https://doi.org/10.1007/978-3-030-44655-0_7

Shipley, T. G., & Bowker, A. (2014). Collecting Legally Defensible Online Evidence. In *Investigating Internet Crimes* (p. 69–97). Elsevier. https://doi.org/10.1016/b978-0-12-407817-8.00004-7

Thomas, A. (2023). Analysis on Cyber Crimes and Preventive Measures. *International Journal for Research in Applied Science and Engineering Technology*, *11*(5), 3738–3744. https://doi.org/10.22214/ijraset.2023.52481

Turrini, E., & Ghosh, S. (2010). A Pragmatic, Experiential Definition of Computer Crimes. In *Cybercrimes: A Multidisciplinary Analysis* (p. 3–23). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-13547-7_1

Yeboah-Ofori, A., & Opoku-Boateng, F. A. (2023). Mitigating cybercrimes in an evolving organizational landscape. *Continuity & Resilience Review*, *5*(1), 53-78. https://doi.org/10.1108/crr-09-2022-0017

Zabarniy, M., Topchiy, V., Shevchenko, A., Lugina, N., & Viacheslav, Y. (2022). Utilizing of the method of statistical data analysis in combating organized crimes. *Revista Amazonia Investiga*, *11*(52), 288–297. https://doi.org/10.34069/ai/2022.52.04.31

Zahoor, R., & Razi, N. (2020). Cyber-Crimes and Cyber Laws of Pakistan: An Overview. *Progressive Research Journal of Arts & Humanities (PRJAH)*, *2*(2), 133–143. https://doi.org/10.51872/prjah.vol2.iss2.43