UDC: 343.9:343.2:343.14:004.9(100)
DOI https://doi.org/10.24144/2307-3322.2025.91.4.41

LEGAL BASIS OF COMBATING CYBERCRIME: CURRENT PROBLEMS AND SOLUTIONS

Kamran K.I.,
Baku State University, Faculty of Law,
Department of Criminal Process, PhD student,
e-mail: kamran.khalilov.isa@bsu.edu.az
ORCID: 0000-0002-0086-009X

Kamran I.K. Legal basis of combating cybercrime: current problems and solutions.

The dynamic evolution of cyberspace has generated complex legal and technological challenges that demand a coordinated international response. As digital communication networks expand beyond national borders, cybercrime has acquired a transboundary dimension that exposes the structural limitations of domestic legal systems. This research undertakes a comprehensive analysis of the legal foundations governing the fight against cybercrime, with particular emphasis on identifying systemic deficiencies, conceptual ambiguities, and enforcement gaps within existing regulatory frameworks. The study examines how the rapid advancement of information and communication technologies has intensified the scale and sophistication of cyber offences, thereby transforming them into a critical threat to global and national security. The multifaceted and highly technical nature of these offences complicates the creation of effective mechanisms for prevention, detection, and prosecution. Consequently, one of the pressing challenges facing law enforcement bodies and international institutions is to refine their understanding of cybercrime, modernize investigative tools, and ensure timely adaptation to emerging threats. By employing a doctrinal and comparative methodology, the research analyzes international conventions, national legislation, and judicial practices to assess their adequacy in addressing cross-border digital crimes. Particular attention is devoted to the legal difficulties surrounding digital evidence gathering, jurisdictional conflicts, and data-sharing procedures. The study argues that strengthening the legal framework, improving institutional specialization, and expanding international cooperation are essential for building a coherent and resilient system of cyber justice. Ultimately, this research contributes to the ongoing academic and policy discourse by proposing scientifically grounded strategies aimed at enhancing legislative harmonization, promoting the use of modern investigative technologies, and fostering a unified global approach to combating cybercrime in an era of accelerating digital transformation.

Key words: cybercrime, prevention, international cooperation, jurisdiction, challenges.

Камран І.К. Правова основа боротьби з кіберзлочинністю: актуальні проблеми та шляхи вирішення.

Динамічна еволюція кіберпростору породила складні правові та технологічні виклики, які вимагають скоординованої міжнародної відповіді. Оскільки мережі цифрового зв'язку розширюються за межі національних кордонів, кіберзлочинність набула транскордонного виміру, що виявляє структурні обмеження національних правових систем. Це дослідження проводить комплексний аналіз правових основ, що регулюють боротьбу з кіберзлочинністю, з особливим акцентом на виявленні системних недоліків, концептуальних неоднозначностей та прогалин у правозастосуванні в рамках існуючих нормативно-правових баз. У дослідженні розглядається, як швидкий розвиток інформаційно-комунікаційних технологій посилив масштаби та складність кіберзлочинів, тим самим перетворивши їх на критичну загрозу глобальній та національній безпеці. Багатогранний та високотехнічний характер цих злочинів ускладнює створення ефективних механізмів запобігання, виявлення та переслідування. Отже, одним із нагальних завдань, що стоять перед правоохоронними органами та міжнародними інституціями, є вдосконалення їхнього розуміння кіберзлочинності, модернізація інструментів розслідування та забезпечення

своєчасної адаптації до нових загроз. Використовуючи доктринальну та порівняльну методологію, дослідження аналізує міжнародні конвенції, національне законодавство та судову практику для оцінки їхньої адекватності у боротьбі з транскордонними цифровими злочинами. Особлива увага приділяється правовим труднощам, пов'язаним зі збором цифрових доказів, юрисдикційними конфліктами та процедурами обміну даними. У дослідженні стверджується, що зміцнення правової бази, покращення інституційної спеціалізації та розширення міжнародної співпраці є важливими для побудови цілісної та стійкої системи кіберправосуддя. Зрештою, це дослідження робить внесок у постійний академічний та політичний дискурс, пропонуючи науково обґрунтовані стратегії, спрямовані на посилення гармонізації законодавства, сприяння використанню сучасних слідчих технологій та сприяння єдиному глобальному підходу до боротьби з кіберзлочинністю в епоху прискореної цифрової трансформації.

Ключові слова: кіберзлочинність, запобігання, міжнародна співпраця, юрисдикція, виклики.

Introduction. The development of technology and the internet has transformed the way people interact, communicate, and work. While these advancements have brought significant benefits, they have also given rise to a new form of criminal activity known as cybercrime. Cybercrime encompasses unlawful activities that are facilitated or carried out through the use of computers, networks, and the internet. Offenders exploit vulnerabilities in computer systems, networks, and online platforms to engage in a wide range of illegal acts, including hacking, phishing, ransomware attacks, data breaches, online fraud, and intellectual property theft. There is no doubt that the financial, social, and psychological consequences of cybercrime have far-reaching impacts on individuals, businesses, governments, and even national security. Due to its cross-border nature and the rapid evolution of technology, cybercrime presents unique legal challenges. Issues such as jurisdiction, difficulties in collecting and preserving digital evidence, and the constant need for updated legislation are only a few of the complex legal aspects associated with this phenomenon. Analyzing these problems assists legal scholars and practitioners in designing more effective frameworks for combating cybercrime [5, p.4]. Furthermore, examining the legal implications of cybercrime helps to identify areas for improving cooperation, harmonizing laws, enhancing information sharing, and developing international frameworks and treaties aimed at simplifying legal processes. By studying the legal consequences of cybercrime, it becomes possible to address existing gaps in legislation, propose necessary reforms, and promote more effective strategies to counter this growing threat.

The main purpose of this research is to examine the legal mechanisms established to combat cybercrime and to identify the key difficulties faced in their implementation. The study aims to analyze both the theoretical and practical dimensions of legal regulation in this field and to explore the role of international cooperation in strengthening the global fight against cybercrime. Special attention is given to inconsistencies between national and international legal frameworks, as well as to the challenges arising from technological advancement that often outpace legislative adaptation. The research also seeks to formulate scientifically grounded recommendations to enhance the efficiency and coherence of legal responses to cyber threats. his study pursues the following specific objectives: to evaluate the effectiveness of intergovernmental cooperation mechanisms; to generalize the legal and institutional challenges of combating cybercrime within different legal systems; to examine the legal obstacles that arise in cross-border evidence collection and information exchange; to develop scientifically grounded recommendations for establishing a more unified and efficient framework for global legal cooperation.

Methodologically, this study employs a combination of doctrinal and comparative legal analysis. The doctrinal approach focuses on a detailed examination of existing international conventions, model laws, and domestic legislation governing the fight against cybercrime. The comparative method allows for the identification of structural differences and common principles across different legal systems, particularly those of countries with advanced cyber legislation. The research further integrates an analytical review of academic literature, judicial practice, and relevant policy documents to obtain a multi-dimensional perspective. A qualitative method of interpretation is used to evaluate legal norms and to develop forward-looking solutions that align with contemporary digital realities.

The state of scientific development of the issue. The study of legal responses to cybercrime has attracted extensive and sustained attention from scholars of both criminal and international law. Prominent researchers such as J. Clough, S. Brenner, P. Csonka, M. Gercke, D. S. Wall, and N. Goodman have examined the evolution of criminal liability in cyberspace, the interplay between national

jurisdictions, and the implications of cross-border digital evidence. Their contributions have shaped the conceptual foundations of cybercrime law, emphasizing the necessity of coherent procedural safeguards and international harmonization. Within this field, significant academic discourse has focused on the Budapest Convention on Cybercrime, often regarded as the cornerstone of international cooperation against cyber threats.

From a normative perspective, the international legal framework for countering cybercrime evolved through several landmark instruments — from the Council of Europe's Recommendation R(89)9 on Computer-Related Crime (1989) and the OECD Guidelines for the Security of Information Systems (1992) to the binding Budapest Convention on Cybercrime (2001) and its Additional Protocol (2003). These acts laid the foundation for global harmonization in defining, investigating, and prosecuting cyber offences. Later instruments, such as the EU Directive 2013/40/EU, further refined procedural standards and reinforced the principle of international cooperation.

Nevertheless, multiple dimensions of the issue remain insufficiently explored. The procedural treatment of digital evidence, the establishment of consistent jurisdictional criteria, and the delineation of universal jurisdiction in cybercrime cases continue to generate legal uncertainty. Furthermore, disparities in national legal frameworks and the absence of a unified approach to data retention and digital forensics hinder efficient international cooperation. This article seeks to bridge these gaps by reassessing the structural and procedural foundations of cybercrime regulation. It emphasizes the need to strengthen investigative capacity, improve interoperability of legal mechanisms, and develop a coherent model for transnational legal collaboration. In doing so, the study contributes to the modernization of criminal procedure in the digital era and highlights the indispensable role of international cooperation in ensuring an effective global response to cybercrime.

Presentation of research material.

Challenges in combating cybercrime.

The rapid development of technology and recent experience clearly illustrate how difficult it is to combat cybercrime. Several factors explain why this struggle poses such challenges for the legal system. First, cybercrime is still a relatively new phenomenon, which makes it difficult to establish fixed patterns of how such offenses are committed [1, p.555]. This lack of clarity prevents the creation of a solid information base to guide the allocation of resources for fighting cybercrime [27]. Although our understanding of the real scale of the problem is limited, it is evident that this is a fast-growing form of criminal activity. Secondly, because cybercrime is a new category of offense, investigative authorities and courts need time to understand and adapt to it. Law enforcement officers and judges, in particular, require regular and specialized training. Since methods of committing cybercrime change rapidly, these institutions must constantly update their knowledge [25, p.140]. Another challenge lies in the absence of a single, clear definition of cybercrime in comparative law. Existing definitions are often ambiguous, and differences in substantive criminal law hinder effective international legal assistance. For this reason, the unification of penalties for cybercrime is crucial. When legislation is outdated and traditional criminal provisions are applied to technology-related offences, punishing offenders is not always possible. Rapid technological progress continuously generates new forms of crime, forcing even states with newly adopted rules to revise and modernize their legislation at the same pace [13].

The nature and collection of evidence also create specific difficulties. Digital evidence differs significantly from traditional evidence, both in form and in the methods required to obtain it. Gathering such evidence is often complex, but it must also be collected in a way that makes it admissible in court and consistent with procedural rules. This underlines the importance of "digital forensics", a field focused on using technical examinations and analyses to extract potential legal evidence. Investigators working in this area therefore need substantial expertise and experience [14, pp.33-34]. Another problem is the fragility of digital evidence, which can be lost at any moment. This makes fast and effective cooperation at both national and international levels essential. For example, when extracting evidence from mobile phones, where crucial information is often stored, investigators and experts apply different methods. Ensuring that these methods are effective and do not damage the evidence should be considered a top priority [15, p.371].

In sum, combating cybercrime is a complex and demanding process that requires constant attention, professional knowledge and practical skills. The problems outlined above represent only part of the challenge. In this context, the main difficulties in addressing cybercrime can be grouped according to their specific nature as follows.

The complex nature of cybercrime.

One of the primary challenges in investigating and prosecuting cybercrimes is the anonymity of offenders. Cybercriminals can exploit information systems without restrictions, thereby gaining worldwide access [6]. Consequently, identifying offenders in cyberspace is particularly difficult, since there are no effective mechanisms to trace their activities. In some cases, the identification of offenders can be attempted using Internet Protocol (IP) Addresses. Nevertheless, obtaining precise location data is not always possible. Offenders may commit crimes using someone else's computer, a device in an internet cafe, or public internet connections in airports, restaurants, or hotels. Furthermore, even if an IP address is detected, problems may arise if service providers either withhold or provide inaccurate information about the offender's identity [11, p. 3]. Another complicating factor is the utilization of specialized communication tools such as TOR (The Onion Router) or Psiphon, which allow users to hide their identities. These systems make IP address tracking almost impossible. For instance, Avalanche, a harmful platform known for producing malware and managing cryptocurrencies worldwide, used a technique called fast flux both to avoid detection and to hide its operators' identities. Through fast flux, data connected to an IP address is rapidly transferred to multiple internet-connected devices through botnets, thereby frequently altering both IP address records and the services generating them [3, p. 117].

No matter how advanced a state's legislative framework on cybercrime may be, such laws remain ineffective unless offenders are successfully detected. In other words, cyber-related provisions cannot be implemented in isolation. To overcome this complication, it has been proposed that users should be required to authenticate their identities when accessing information systems. However,human rights advocates claim that these obligations infringe upon individuals' rights to privacy and personal autonomy [11, p. 4]. A further significant challenge concerns acquisition and preservation of digital evidence by law enforcement agencies. In order to determine the actual offender, it is essential not only to assign responsibility to an individual but also to substantiate the offense through authentic evidence. Unlike conventional crimes, the types of evidence and methods of collection in cybercrime cases are significantly distinct. The "crime scene" in such instances is the information system itself [365]. Consequently, evidence of the violation must be traced within these systems. However, the intrinsic character of such immaterial cyber evidence is inherently fragile and may be partially or completely lost at any time [366]. Furthermore, such evidence can be easily modified, encrypted, or otherwise manipulated, creating further challenges for investigators [21, p. 32].

Additionally, it is evident today that data storage capacity of information systems, which are the precise tools used in the commission of cybercrimes, has increased significantly. Consequently, investigators are frequently obliged to search through hundreds of thousands of data entries to determine relevant evidence. In some instances, information related to cybercrimes may be scattered throughout information systems located in multiple jurisdictions. This situation creates new challenges for law enforcement agencies and considerably complicates the process of evidence collection. On the other hand, data may be encrypted, making it impossible for law enforcement authorities to access information without decryption. İn fact, substantial time is often required to decipher passwords. Therefore, in this cyber domain, obtaining and analyzing evidence requires advanced knowledge in digital forensics as well as substantial IT proficiency [10, p. 95].

Jurisdictional issues.

Another major challenge in combating cybercrime concerns the identification of the offender's whereabouts and determining under which legal framework the individual should be subjected to liability. In this regard, the definition of jurisdiction becomes vitally significant. In international law, jurisdiction is generally understood as the authority of a state to exercise power or control over individuals and entities. From this perspective, jurisdiction traditionally encompasses three principal dimensions: legislative, executive, and judicial authority. These three classical forms of jurisdiction have historically been grounded in territorial principle [20, p. 88]. Nevertheless, in these circumstances, the territorial principle proves insufficient, and it is complemented with other doctrines such as the nationality principle, the protective principle, or the principle of universal jurisdiction. According to the territorial principle, a state enforces its authority within its geographical boundaries, which cover terrestrial, maritime, aerial, and extraterrestrial domains. In other words, the government possesses the jurisdiction to determine whether an act constitutes a criminal offense within these domains, to identify the competent courts, and to specify the relevant legislation [16]. States, therefore, may not generally extend this jurisdiction within the legal domain of another sovereign state. These traditional forms of

jurisdiction have fixed firmly determined and explicit boundaries across terrestrial, maritime, aerial, and extraterrestrial domains. When a conventional crime is committed within these territories, identifying the place of commission and, ultimately, determining the responsible jurisdiction is usually not complicated. On the other hand, cybercrimes are committed in cyberspace, which transcends territorial boundaries and falls under no single state's sovereignty. Such offenses can be perpetrated by individuals located anywhere in the world, employing only a networked computer from a remote location. This situation raises the fundamental question of the place of commission of the crime in order to identify the relevant legislation and the authorized judicial body. The problem is intensified by the intrinsic challenge of precisely delineating actions that amount to a cybercrime. Jurisdictional issues become particularly complex when the main components of a cybercrime are distributed across multiple states [9, p. 45].

The determination of which elements constitute a criminal act (such as motive, casual relationship etc.) and the identification of the location where the crime is considered to have been committed represent distinct matters. For instance, in crimes involving content disseminated via information technologies, such as offensive speech or child pornography, authorities face challenges in determining the location of the offense and the location of the associated network. Moreover, content may begin to be uploaded in one jurisdiction and be completed in another, or an offender may create content in one country while making it accessible to the public in another. Consequently, a cyber activity can be subject to multiple national jurisdictions. Since, there is no international authority or judicial body capable of resolving such issues, states endeavor to address the problem through the jurisdictional provisions incorporated within their national legal frameworks [2]. Currently, there is no specialized international body or court addressing cybercrime. The jurisdiction of the International Criminal Court (ICC) encompasses crimes listed under Article 5 of the Roma Statute, specifically genocide, war crimes, crimes against humanity, and the crime of aggression that threatens the international community [30]. In this regard, cybercrimes are not explicitly incorporated within the Roma Statute. Nevertheless, some scholars argue that cyber activities may create new ways of committing criminal acts, thus allowing or supporting their execution. Therefore, these actions might be subject to the jurisdiction of Article 414 of the ICC. At first glance, it seems that cyber activities could be considered within the framework of an act of aggression [4, p. 320]. To qualify as an act of aggression, a cyberattack must meet certain criteria. As stated in paragraph 1 of Article 8 of the Roma Statute, the crime of aggression stipulates that the act be executed by a person with the authority to control and oversee effectively the military and political affairs of a state. This leadership requirement is rarely met in the context of cyberattacks. Nonetheless, in rare circumstances, such as extensive denial-of-service (DoS) attacks, this criterion might be satisfied. For instance, during the 2008 confrontation, Russian affiliated groups conducted DoS assaults against the Georgian government, thereby incapacitating its capacity to convey information to the public [26, p. 200).

In international law, two principal mechanisms enable either international tribunals or national courts to assert jurisdiction over cybercrime, namely the principle of universal jurisdiction and the principle of complementarity. In the context of transnational offenses requiring cross-border cooperation, the universality principle assumes particular significance [26, p. 223]. According to this principle, states may assert jurisdiction over crimes that threaten the international community as a whole, regardless of where the crime was committed or the nationality of perpetrator or victim. In other words, the principle of universal jurisdiction authorizes a state to prosecute offenses that it would not otherwise have jurisdiction over under terrioriality, personality, or protective principles. This principle has historically been invoked in the prosecution of organized transnational crimes against humanity, including piracy and transnational terrorism [19, p. 126]. The principle of universality enables any state, whether through international or national courts, to assert jurisdiction over offenders, thereby offering a potential solution to the challenges posed by cybercrime. Piracy, for instance, has been characterized as "hostis humani generis" , an offense against all humankind, and may be prosecuted within the jurisdiction where it occurs. According to the 1982 United Nations Convention on the Law of the Sea (UNCLOS) and established principles of customary international law, acts of piracy committed on international waters may be prosecuted by any state [31]. Analogously, cyber offenders may be considered the enemies of humanity, while cyberspace can be compared to the high seas. The justification for applying universal jurisdiction to piracy rests on the premise that international commerce is endangered, with large-scale DoS attacks having the potential to incapacitate or substantially disrupt critical commercial websites. Consequently, cybercrimes of this nature should be prioritized under the framework of universal jurisdiction. Nevertheless, delineating the scope of cybercrimes may pose challenges to the application

of the universality principle. If the scope of such offenses is carefully defined, however, it can serve as a deterrent in combating cybercrime. According to the complementarity principle, national courts hold primary responsibility for exercising jurisdiction over crimes. The principle was emphasized prior to the Rome Conference with the notion of the " complementarity of international criminal adjudication with national criminal justice" [12, p. 171]. However, when national courts are either unwilling or lack the necessary technical capacity to prosecute an offense, the International Criminal Court (ICC) has the authority to assume jurisdiction over such cases. In this regard, the principle of complementarity respects the national sovereignty of states. It also addresses challenges arising from certain states' failure and refusal to prosecute cybercriminals or to extradite them. Nevertheless, the principle does not entirely resolve cybercrime issues that fall within the jurisdiction of multiple states' legal systems. In such circumstances, effective resolution may require the involvement of a supranational court or an international governing authority.

Challenges in international cooperation.

Another significant challenge in countering cybercrime is the absence of effective transnational cooperation. The principal aim of international collaboration is to prevent offenders who commit crimes across multiple legal jurisdictions from evading accountability. Effective crime prevention necessitates anticipating the penalties that offenders will face for their actions. A criminal act may endanger not only the national security of the state in which they occur but also that of other nations. In the context of cybercrime, offences frequently transcend national boundaries, thereby heightening the probability that perpetrators may evade prosecution. Consequently, all states and international entities must collaborate to enhance transnational cooperation. Even if states establish comprehensive and effective substantive and procedural frameworks addressing cyber crimes, such measures alone remain inadequate. The suppression of these crimes fundamentally relies on mechanisms of intergovernmental collaboration. As emphasized in scholarly discourse, the struggle against cybercrime " must be global in nature or it will have no meaning at all " [23, p. 188]. In other words, international collaboration is considered an indispensable requirement. If even a few states do not participate, cybercriminals may exploit countries not engaged in extradition or mutual legal assistance agreements as safe havens, continuing their illegal activities from those jurisdictions. Several key factors contribute to the challenges of international cooperation, the three most critical being: A) differences in national legal systems; B) gaps and incompleteness in international treaties; C) excessively lengthy and time-consuming procedural rules.

A) Differences in national legal systems:

Initially, when discussing distinctions in legal systems, it can be noted that these systems evolve in response to the particular needs and realities of societies. Laws represent a diverse range of societal factors, including religion, culture, history, sociology, and geography. Consequently, substantive and procedural criminal legislation vary significantly across states [22]. The issue becomes even more intricate in the context of cybercrime. From a substantive law perspective, determining which actions constitute a criminal offense differs significantly between jurisdictions. As discussed in the first chapter, there is no overarching agreement regarding the definition and scope of a crime. An act that is considered criminal in the victim's country may not be recognized as such in the perpetrator's jurisdiction, or it may be classified differently. For instance, while "national-socialist" propaganda is punishable as a criminal offense in Germany and Austria, it is generally protected under freedom of expression in the United States, Australia, and Canada [32. p. 113]. Similarly, acts of hate speech constitute a punishable offense in many European countries, whereas it is often safeguarded as free expression in the United States. A notable illustration of this disparity is the Yahoo! v. LICRA case. In this case, Yahoo! provided access to websites offering Nazi-related materials, including photographs,sale, exchange, or display of Third Reich memorabilia, in violation of French criminal law. Consequently, in 2000, the French non-profit organization International League Against Racism and Anti- Semitism (LICRA) filed a lawsuit against Yahoo!. As a result, the Paris court ruled that Yahoo! must take all necessary measures to prevent access to Nazi-related materials. In compliance with the court's decision, Yahoo! eliminated all such content from its French site (www.yahoo.fr). However, the Paris Court subsequently required that the same content be removed from Yahoo!'s global platform accessible to French users. Yahoo! rejected this request. Subsequently, the case was submitted to the United States District Court for the Northern District of California, which argued that enforcing the Paris Court's decision on the global site (www.yahoo.com) would contravene the constitutional protection of freedom of expression guaranteed under the U.S. Constitution. The court ultimately ruled that the Paris Court's order was incompatible with

the U.S. Constitution and, therefore, unenforceable within the jurisdiction of the United States [24, pp. 214–220]. Just as substantive criminal laws vary among nations, the procedural frameworks that regulate criminal investigations and prosecutions also demonstrate significant differences. Methods for investigating crimes, conducting trials, and collecting evidence may be lawful and effective within one jurisdiction, but inadequate or illegal in another. These discrepancies frequently lead to conflicts between national legal systems. For instance, remote search measures are regarded as legitimate procedures for obtaining criminal evidence in the United Kingdom and the United States. Conversely, in other countries, similar practices may be deemed illegal and constitute a violation of individual privacy rights [28]. In fact, one of the most critical challenges in cybercrime investigation concerns the storage and preservation of data, as various states impose diverse requirements regarding data retention.

Variations in national criminal law systems often lead to inconsistencies and conflicts in provisions related to cybercrime, thereby impeding international cooperation. Dual criminality constitutes a fundamental condition for the implementation of legal assistance and extradition procedures. According to this principle, the offense forming the basis of a request for legal assistance must be recognized as a crime under the criminal laws of both the requesting and requested states. Noncompliance with this requirement can significantly impede operational procedures, such as evidence collection, conducted within the framework of international collaboration [7, p. 255]. Furthermore, the concept of "jurisdictional arbitrage" becomes particularly relevant in this context. Cybercriminals may reside and operate in states that either fail to criminalize certain cyber offenses or prescribe only minimal sanctions for such conduct. In other words, an act deemed unlawful in one country may not constitute crime in another, complicating prosecution efforts and obstructing international cooperation [8, p. 477]. To address this challenge, it is essential for states to pursue harmonization of their cybercrime legislation. However, the process of alignment is complicated by diverse factors, including states' political structures, histories, cultures, social dynamics, and legal traditions. The principle of "one-size-fits-all" is not applicable to cybercrime. Consequently, combating such offenses requires tailored approaches that consider the unique domestic conditions of each state. It is important to emphasize that legislative harmonization does not aim to enforce uniformity. Rather, the goal is to achieve functional complementarity. In other words, national and regional differences should be minimized to the extent possible, while ensuring that enforcement mechanisms operate with both effectiveness and efficiency.

B Incompleteness of international treaties:

Extradition and mutual legal assistance constitute the most essential mechanisms for international cooperation among states. Over recent years, the scope of mutual legal assistance, which was previously narrow, has expanded substantially. Today, legal assistance comprises an extensive spectrum of activities, including the provision of information, transmission of data regarding criminal offenses, delivery of court decisions and documents related to judicial proceedings, examining of witnesses, experts, and defendants, execution of searches and seizures for evidentiary purposes, transfer of objects or documents, and the extradition of detained persons to another state. In the absence of intergovernmental agreements, states are not legally obligated under international law to cooperate with other countries in matters related to cybercrime or any other offenses [17, p. 220]. This reveals a significant gap in international law. In other words, these legal assistance and extradition processes are implemented exclusively through bilateral or multilateral treaties concluded between states, for instance, the Council of Europe's Convention on Cybercrime or the European Convention on Mutual Assistance in Criminal Matters. Nevertheless, to date, no comprehensive international treaty specifically addressing cybercrime. The effectiveness of lateral and multilateral regional agreements is limited to the participating states. Consequently, these limitations pose substantial challenges to combating cybercrime at a global level.

A notable instance illustrates the absence of agreements on international cooperation within the cybercrime context in the 2000 case involving Gorshkov and Ivanov. Russian hackers Vasiliy Gorshkov and Aleksey Ivanov illegally accessed the IT systems of several American companies, extrafiltrated their data, and subsequently conducted extortion attempts [29]. Due to the lack of an extradition treaty between the United States and Russia, it was not possible for the Russian authorities to surrender the suspects. Consequently, the Federal Bureau of investigation (FBI) arranged the transfer of the suspects to the United States to enable criminal investigation and subsequent prosecution. FBI agents employed a fictitious company called "Invita" to bring the suspects to the U.S. , where, as part of an interview process, they were asked to display hacking capabilities by typing on a network set up by the FBI. Prior to this, the FBI had installed surveillance programs on the computers that the suspects would use in the

United States, allowing it to obtain passwords and data from computers located in Russia. Utilizing the information and evidence retrieved from these Russian-based computers, the authorities were able to prosecute and detain the suspects. The Russian government protested the operation and demanded the surrender of the offenders, however, in the absence of a formal agreement, the U.S. authorities declined the request [18] .

C) The excessive length and complexity of procedural rules:

The procedural framework for extradition and international judicial cooperation in cases involving cybercrime remains excessively lengthy and time-consuming. Requests related to extradition of mutual legal assistance in cybercrime matters are processed through conventional diplomatic or judicial channels in both states. These mechanisms, such as legal transactions, translation of official documents, and other formal procedures are often bureaucratically and inefficient. Consequently, they prove inadequate in addressing cybercrimes, which advance at a remarkable rate and frequently transcend jurisdictional boundaries. In other words, the conventional regime of international judicial cooperation is often inadequate to the dynamic nature of cybercrime and frequently fails to provide timely or effective support in response to requests for cooperation. For instance, The United States, one of the world's most technologically advanced nations, reportedly requires an average of ten months or more to respond to other countries' requests concerning the database of cyber offenders [26, p. 207].

If a crime involves offenders or connections spanning multiple countries, the procedure for securing mutual legal assistance tends to become significantly prolonged. This extended duration elevates the probability of losing crucial evidence and information related to the crime. Therefore, conventional frameworks of international collaboration must be replaced with more efficient and rapid methods. For instance, the establishment of 7/24 international emergency communication networks could facilitate direct interaction between investigators and experts from different jurisdictions. Beyond the limitations of conventional international cooperation frameworks, multiple operational challenges impede efficient mutual legal assistance. These include rejection of requests due to minor deficiencies in submitted documentation, the absence of direct interaction between judicial bodies and justice ministries concerning document transmission, insufficient legal knowledge among law enforcement officials, inadequately conducted investigative procedures, and limited foreign language among personnel involved. All these factors collectively impede the legal assistance process and weaken the overall effectiveness of cross-border collaboration in criminal justice.

Conclusion.

Efforts to overcome the challenges encountered in combating cybercrime should be enacted at both national and international levels. At national level, the foundation for combating cybercrime is embedded in a nation's criminal and procedural legislation. In the absence of an effective regulatory framework addressing cybercriminal activities, states risk becoming safe havens for cybercriminals. Therefore, as cybercrime continues to evolve, states should simultaneously reform, enhance, and adapt their national substantive and procedural criminal laws to effectively address these emerging threats. Furthermore, traditional instruments of criminal investigation and prosecution are largely inadequate in dealing with cybercrime. Specifically, the collection, the preservation, and assessment of digital evidence require the establishment of specialized digital forensic laboratories and a comprehensive forensic infrastructure. Therefore, law enforcement agencies should develop innovative and rapid methods for investigating and prosecuting cyber offences, while guaranteeing sufficient technical capacity and operational readiness for cybercrime prevention.

Furthermore, to effectively combat cybercrime, the formation of specialized bodies focused on cybersecurity oversight and enforcement is indispensable. In addition, states must enhance their information technology infrastructures and implement the necessary technical measures to ensure cyber resilience. At this point, it is essential to design and execute comprehensive projects, as well as to develop strategic plans targeting the protection of cybersecurity and privacy while preventing cyberattacks. In addition, a substantial proportion of cybercrimes remain unreported. This underreporting is largely attributable to victims' awareness of being subjected to cyber attacks that they have been targeted or their unfamiliarity with the proper reporting procedures. Furthermore, certain companies and institutions often withhold information regarding cyber incidents owing to apprehension about possible reputational damage. Consequently, targeted research initiatives and public awareness campaigns should be implemented to educate citizens on cybercrime and the appropriate mechanisms for reporting such offences. At national level, efficient collaboration among law enforcement agencies, both internally

and with the private sector is essential. Internet service providers, in particular, play a critical role in ensuring access to relevant data. On one hand, service providers must assist law enforcement authorities in tracing perpetrators, while on the other hand, they are obliged to protect individual rights and privacy, preventing any potential misuse of sensitive information.

Combating cybercrime on a global scale is of equally vital importance. In other words, while national legislation constitutes the foundation of the fight against cybercrime, international law represents its culmination. A global crime necessitates a global response. National laws alone frequently prove inadequate for effectively tackling transnational cyber offences. In this context, there is a pressing need for a legally binding international agreement to govern and enhance international cooperation in this field. The most prominent and authoritative platform for achieving this objective is the United Nations (UN). Within the UN framework, the principal purpose of such an international convention should be to harmonize and align both substantive and procedural criminal legislation of member states concerning cybercrime. This would ensure the implementation of the principle of dual criminality, which serves as a fundamental prerequisite for international cooperation, and would help eliminate discrepancies among states regarding the investigation and prosecution of cyber offences. Traditional forms of international cooperation are largely incompatible with the inherent nature of cybercrime, as they often prove to be inefficient and excessively time-consuming. The fight against cybercrime requires effective, rapid, and sophisticated mechanisms of international collaboration. Transnational cyber offences frequently fall within the jurisdiction of multiple states, yet there is currently no international body or legal norm capable of adjudicating jurisdictional conflicts. Furthermore, cybercrime does not appear to fall within the jurisdiction of the International Criminal Court (ICC). Two potential solutions can be proposed for this issue. The first is to include cybercrime as a fifth core international crime within the jurisdiction of the ICC, alongside war crimes, crimes against humanity, genocide, and the crime of aggression. The second is to establish a specialized international tribunal on cybercrime, modeled after the ICC, with exclusive competence over such offences. Moreover, international cooperation should not be limited to judicial collaboration but must also encompass police cooperation. Institutions such as INTERPOL, EUROPOL, ASEANAPOL, and AMERIPOL play an indispensable role in facilitating transnational law enforcement collaboration. It should also be emphasized that there exists a substantial digital divide among developed, developing, and underdeveloped countries in terms of information technology capacity. Bridging this gap and promoting the transfer of technological knowledge are essential for sustaining global cybersecurity and ensuring a more effective worldwide response to cybercrime.

REFERENCES:

1. Akbulut, B.B. (2020). Cyber Crimes, Selcuk University *Faculty of Law Journal, Millennium Gift*, Volume 8, Issue 1-2, – 2000.
2. Albert I. Aldesco. (2002). The Demise of Anonymity: A Constitutional Challenge to the Convention on Cybercrime, *Loyola of Los Angeles Entertainment Law Review*, Vol.23, No. 1, p. 89.
3. Bell, R.E. (2002) The Prosecution of Computer Crime, *Journal of Financial Crime*, Vol. 9, No. 4, p. 314.
4. Cammack, C. (2011). The Stuxnet Worm and Potential Prosecution by the International Criminal Court under the Newly Defined Crime of Aggression, *Tulane Journal of International & Comparative Law,* Vol. 20, No. 1, p. 319–324.
5. Clough, J. (2015). Principles of Cybercrime. Second edition. Cambridge University Press, p. 513.
6. Clough, J. (2011). Cybercrime. *Commonwealth Law Bulletin,* Vol. 37, No. 4, p. 673.
7. Clough, J. (2014). A World of Difference: The Budapest Convention On Cybercrime And The Challenges Of Harmonisation, *Monash University Law Review*, Vol. 40, No. 1, p. 701.
8. Csonka, P. (2006). The Council of Europe's Convention on Cyber-crime and Other European Initiatives, *Revue İnternationale de Droit Penál* , Vol. 77, No. 3, p. 620.
9. David L. Speer. (2000). Redefining Borders: The Challenges of Cybercrime, Crime, *Law and Social Change*, Vol. 34, No. 3, p. 260.
10. Ehuan, A. (2010). Cybercrime and Law Enforcement Cooperation, CyberForensic Understanding Information Security Investigations, Ed. Jennifer Bayuk, Germany, Springer, p. 138.

11. Emmanuel Femi Gbenga Ajayi. (2016). Challenges to Enforcement of Cyber-Crimes Laws and Policy, *Journal of Internet and Information Systems*, Vol. 6, No. 1, p. 4.
12. Erdal, S. (2010). Uluslararası Ceza Mahkemesinin Ulus-Devlet Egemenliğine Etkisi, Selçuk Üniversitesi Hukuk Fakültesi Dergisi , C.XVIII, S. 1, s. 195.
13. Gregor U. (2006). Criminalising Computer Misconduct: Some Legal and Philosophical Problems, 14 Asia Pac. L. Rev. 95, p. 99.
14. Khalilov, K., & Abbasova F. (2024). Modern methodology of digital forensics: The role of technology in digital criminal prosecution. Qanun Nəşriyyatı, № 05 (355), s. 33–44.
15. Khalilov, K. (2025). Obtaining digital evidence and protecting personal data in the preliminary investigation of cybercrimes: interaction and comparative analysis. Doktorantların və gənc tədqiqatçıların XXVII r. elmi konfransı (NASCO XXVII). Materiallar toplusu – II hissə, s. 369–374.
16. Henriksen, A. (2019). International Law, 2. bs., United Kingdom, Oxford Universty Press, p. 85.
17. Inger Marie S. (2018). Cybercrime Law, Digital Forensics, Ed.André Årnes, Hoboken John Wiley & Sons, p. 111.
18. Jean-Baptiste M. (2019). The limits of Subjective Territorial Jurisdiction in the Context of Cybercrime, ERA Forum, Vol. 19., No. 3, p. 384.
19. Keçeligl, M.D. (2018). Evrensel Yargı Yetkisi: Ceza Hukuku Bağlamında Evrensellik İlkesine Bakış, Terazi Hukuk Dergisi, C.XIII, s. 143.
20. Khalilov, K. (2024). Extraterritorial Jurisdiction of the ECHR in the Context of Analysis of Relevant Cases: Which Model Is Effective? 10, Scopus Preview, Baku St. U. L.Rev.84, p. 84–120.
21. Kim-Kwang R.C. (2008). Organised Crime groups in Cyberspace: a Typology", *Trends Organ Crim*, Vol.11, No. 3, p. 287.
22. Matthew R.Z. (2001). International Computer Crimes, General Report, Revue internationale de droit pénal, Vol. 72, No. 3, p. 827.
23. Murat V.D. (2018). Bilişim Suçları ve İnternet İletişim Hukuku, 7. bs., Ankara, Seçkin Yayınları, s. 256.
24. Okoniewski, E.A. (2002). Yahoo!, Inc. v. LICRA: The French Challenge to Free Expression on the Internet, American University International Law Review, Vol. 18., No. 1, p. 380.
25. Özgür U. & Yasin B. (2004). Bilişim-İletişim Teknolojileri ve Ceza Hukuku, İnternet ve Hukuk (derleyen Yeşim M. Atamer), İstanbul Bilgi Üniversitesi Yayınları, İstanbul, s. 423.
26. Perloff-Giles, A. (2018). Transnational Cyber Offenses: Overcoming Jurisdictional Challenges, *The Yale Journal of International Law*, Vol. 43, No. 1, p. 227.
27. Susan W.B. (2004). Toward a Criminal Law for Cyberspace: A New Model of Law Enforcement?, 30, Rutgers Computer & Tech. L.J. 1, p. 33.
28. Susan W. B. (2012). Law, Dissonance, and Remote Computer Searches, *North Carolina Journal of Law & Technology*, Vol. 14, No. 1, p. 124.
29. Susan W. Brenner, Joseph J. Schwerha IV. (2002). Transnational Evidence Gathering and Local Prosecution of International Cybercrime, *The John Marshall Journal of Information Technology & Privacy Law*, Vol. 20, No. 3, p. 347-348.
30. Ulusoy, O. (2008). Uluslararası Ceza Mahkemesi, Ed. Utku Kılınç, İzmir, Etki Matbaacılık Yayıncılık, s. 22–29.
31. United Nations Convention on the Law of the Sea. Available at: https://www.un.org/depts/los/convention_agreements/texts/unclos/unclos_e.pdf [accessed Sep 05, 2025].
32. Veli Özer Ö. (2002). İnternet Kullanımında Ortaya Çıkabilecek Bazı Ceza Hukuku Sorunları, DEÜHFD, C.IV, S. 1., s. 130.