Operative-Search Activities in Combating New Forms of Digital Organised Crime

Submitted: 1 September 2025
Reviewed: 29 November 2025
Revised: 15 December 2025
Accepted: 18 December 2025

Dauren Kozhabekov[*]
https://orcid.org/0009-0006-2694-0967
Aliya Bayseitova[**]
https://orcid.org/0000-0002-1648-9432
Aidar Saitbekov[***]
https://orcid.org/0009-0009-6132-490X
Assel Kassymova[****]
https://orcid.org/0000-0001-9333-4146
Elvira Alimova[*****]
https://orcid.org/0000-0002-0164-6888

Article submitted to peer blind review

DOI: https://doi.org/10.26512/lstr.v18i2.59526

Abstract

[Purpose] The research presents a fundamental theoretical and empirical study of the issues of operational and investigative activities in the context of countering the latest forms of organised crime in the digital space.

[Methodology/approach/design] A scientific analysis is made of the conceptual and categorical apparatus and essential characteristics of operational and investigative measures used to detect, document and suppress criminal activity in the context of the digital transformation of society. The methodological foundations and structural elements of the system of operational and investigative measures are examined, with due regard for

[*]Master, Doctoral Student at the Almaty Academy of the Ministry of Internal Affairs of the Republic of Kazakhstan by M. Esbolatov, 050060, 29 Utepov Str., Almaty, Republic of Kazakhstan. E-mail: d_kozhabekov@outlook.com.

[**]Full Doctor, Head of the Almaty Academy of the Ministry of Internal Affairs of the Republic of Kazakhstan by M. Esbolatov, 050060, 29 Utepov Str., Almaty, Republic of Kazakhstan. E-mail: bayseitova.a08@outlook.com.

[***]Full Doctor, Professor at the Almaty Academy of the Ministry of Internal Affairs of the Republic of Kazakhstan by M. Esbolatov, 050060, 29 Utepov Str., Almaty, Republic of Kazakhstan. E-mail: aidar_saitbekov@hotmail.com.

[****]PhD, Senior Prosecutor at the Prosecutor General's Office of the Republic of Kazakhstan, 010000, 14 Mangilik El Ave., Astana, Republic of Kazakhstan. E-mail: asselkassymova6@gmail.com.

[*****]PhD, Academic Secretary at the Almaty Academy of the Ministry of Internal Affairs of the Republic of Kazakhstan by M. Esbolatov, 050060, 29 Utepov Str., Almaty, Republic of Kazakhstan. E-mail: alimova@hotmail.com.

the specifics of the digital environment and the peculiarities of modern organised criminal groups
[Findings] On the basis of a comprehensive comparative legal analysis of Kazakh and international legislation, the peculiarities of regulatory and legal regulation of the activities of operational and investigative units in the field of combating organised crime in the digital space are revealed. Key areas for modernisation of criminal, criminal procedure and operational search legislation are identified to improve the efficiency of law enforcement in the context of digitalisation of crime. In the context of international cooperation, the current state of interaction between law enforcement agencies of different countries in combating transnational organised crime is analysed, promising areas for the development of interstate cooperation and mechanisms for improving its effectiveness are identified. Specific recommendations are formulated for optimising the use of special technical means and information technologies in the process of documenting the illegal activities of organised criminal groups. As a result of the study, the role and importance of operational and investigative units of internal affairs bodies in the system of combating organised crime in the digital space are defined, and scientifically sound proposals for improving their activities are developed.
[Practical implications] The recommendations are formulated for modernising the tactics and methods of conducting operational and investigative measures aimed at identifying and documenting new forms of criminal activity in the digital environment. A set of organisational and legal measures is proposed to improve the effectiveness of preventive activities of law enforcement agencies in the field of combating organised crime in the context of the digital transformation of society.
[Originality/value] The study provides a longitudinal analysis of cybercrime trends in relation to major global events, and links the rise in cyber incidents to geopolitical and economic disruptions.

Keywords: Monitoring. Investigation. International Cooperation. Documentation. Evidence.

INTRODUCTION

The rapid development of digital technologies and global digitalisation of social relations has significantly transformed organised criminal activity. Organised criminal groups actively use advanced technological capabilities to enhance illegal activities, presenting serious challenges for law enforcement agencies of the Republic of Kazakhstan and other countries. These criminal groups demonstrate high technological adaptability and rapidly modify tactics in response to law enforcement countermeasures.

The challenge of combating digital organised crime is particularly relevant within Kazakhstan's legal framework. The foundational legislation governing operative-search work requires significant adaptation to address digital crime specifics. Current legal provisions define operative-search activities as "measures conducted by authorised state bodies within their competence using public and

covert methods" but lack specific provisions addressing digital investigation techniques (Law "On Operational and Investigative Activities", 1994).

Statistical data from the Committee on Legal Statistics and Special Accounts of the Prosecutor General's Office of the Republic of Kazakhstan (2023) reveals the scope of the problem. In 2023, law enforcement agencies registered 21,358 cybercrimes, with organised criminal groups responsible for approximately 17% of these offenses. The detection rate for such crimes reached only 43%, significantly lower than the average 67% rate for conventional crimes, demonstrating the challenges in applying traditional operative-search methods to digital environments.

Kazakhstan's procedural legislation defines evidence as "legally obtained factual data", but provides insufficient guidance on digital evidence collection and authentication procedures. Current provisions regulating the use of scientific and technical means in the process of proof offer only general guidance inadequate for digital forensics complexities (Criminal Procedure Code…, 2014). This legislative gap creates significant challenges for operative-search units investigating digital organised crime.

Research by A. Khamzin et al. (2023) demonstrates that traditional operative-search methods require significant adaptation to digital environments, as classical approaches prove ineffective in investigating cybercrime. M. Bolatbek et al. (2024) highlight that modern criminal groups actively use cryptocurrencies, the darknet, and encryption technologies to conceal activities.

The transnational nature of modern cybercrime necessitates international cooperation between law enforcement agencies (DZIUBYNSKYI et al., 2024). A study by W. Van der Wagen and W. Pieters (2020) shows that digital crime investigation effectiveness increases significantly through prompt information exchange and international coordination. Kazakhstan has strengthened this cooperation through participation in regional initiatives like the Shanghai Cooperation Organisation (SCO) and the Collective Security Treaty Organisation (CSTO), which established specific protocols for information sharing on digital crimes.

The introduction of specialised technologies has become crucial in combating digital crime (SMAILOV et al., 2025a). Research by C. Horan and H. Saiedian (2021) reveals prospects for using artificial intelligence (AI) and machine learning systems to analyse digital traces, automating suspicious activity identification. Implementing these technologies requires legal amendments to Kazakhstan's operative-search legislation, particularly regarding electronic evidence admissibility.

In recognition of these challenges, Kazakhstan established the Department for Combating Cybercrime within the Ministry of Internal Affairs (Adyrna.kz,

2024). This specialised unit focuses on investigating organised criminal activity in digital environments but faces significant challenges regarding the legal framework for operative-search activities in cyberspace.

Despite numerous studies on operative-search activities, combating new forms of digital organised crime remains insufficiently developed in Kazakhstan's legal context. Particular gaps exist in the legal regulation of special technical means and information technologies in operative-search activities, procedures for documenting cybercrimes, and mechanisms for international cooperation in this area.

The purpose of this study is to develop theoretical provisions and practical recommendations for improving operative-search activities in combating new forms of digital organised crime in the Republic of Kazakhstan, with particular focus on addressing legislative gaps, enhancing electronic evidence collection procedures, and strengthening international cooperation mechanisms.

To achieve this goal, it was necessary to solve the following tasks:

1.To analyse the current state and trends in the development of digital organised crime.

2.To study the peculiarities of legal regulation of operational and investigative activities in the digital environment.

3.To identify problematic aspects of the use of operational and investigative measures in combating new forms of organised crime.

4.To develop proposals for improving the legal framework and practice of operational and investigative units.

MATERIALS AND METHODS

The study was conducted in 2023-2024 using a comprehensive approach to the study of operational and investigative activities in combating digital organised crime. The research methodology included analysis of normative legal acts, comparative legal research, and statistical analysis of cybercrime data from the Committee on Legal Statistics and Special Accounts of the Prosecutor General's Office of the Republic of Kazakhstan (2019-2023).

The regulatory framework of the study included the following acts of the Republic of Kazakhstan: The Criminal Procedure Code (2014), particularly Articles 111-126 on evidence and Articles 231-245 on covert investigative actions; with focus on Articles 4-6 on information security measures; the Law No. 54-XIII "On Operational and Investigative Activities" (1994), examining Article 6 on types of operative-search measures and Article 10 on technical means usage.

In the international legal aspect, the Budapest Convention on Cybercrime (2001), with emphasis on Articles 14-21 concerning electronic evidence collection; the Council of Europe Convention on Laundering, Search, Seizure and

Confiscation of the Proceeds from Crime and on the Financing of Terrorism (2005); and the United Nations (UN) Convention against Transnational Organised Crime (2004) were analysed.

For the comparative analysis, legislation from three countries was examined using structured criteria: comprehensiveness of digital evidence regulation, institutional frameworks, and technical requirements. Singapore was chosen as a global leader in cybersecurity (Cybersecurity Act, 2018). Estonia represents the European approach to digital security (Cybersecurity Act, 2023). The experience of Uzbekistan (Law "On Operational Investigative Activities", 2012) is important for the analysis due to the similarity of legal systems with Kazakhstan.

An essential part of the study was the analysis of the normative legal framework, including the Normative Resolutions of the Supreme Court of the Republic of Kazakhstan "On Amendments and Supplements to Certain Regulatory Resolutions of the Supreme Court of the Republic of Kazakhstan on Criminal and Criminal Procedure Legislation" (2018) and "On Certain Issues of Sanctioning Preventive Measures" (2020).

The research also incorporated analysis of statistical data on cybercrime investigation effectiveness from the Committee on Legal Statistics (2019-2023), examining detection rates, investigation timeframes, and prosecution outcomes for digital organised crime cases.

The methodological basis of the study is the fundamental provisions of the theory of operational and investigative activities, criminal procedure and forensics. The study was conducted using a systematic approach, which made it possible to consider operational and investigative activities as an integral system of measures to counter digital organised crime. The comparative legal method was used to compare the legislation of different countries in the field of regulating operational and investigative activities and to identify common trends and features.

RESULTS

Methods of Detecting and Documenting Digital Crime

In the context of the rapid digitalisation of society, operational and investigative activities undergo fundamental changes in approaches to detecting and documenting crimes. Modern organised criminal groups are actively using digital technologies, which requires the introduction of new operational methods.

The process of detecting digital crime begins with comprehensive monitoring of the digital space. Law enforcement agencies systematically monitor network activity using specialised software to analyse large amounts of data

(MEHLA and MEHLA, 2024). Particular attention is paid to monitoring the darknet and closed online communities, where organised criminal groups often coordinate their activities. According to research, about 60% of serious cybercrime is linked to activity in the darknet (Di Nicola, 2022). An important step is the collection and analysis of digital traces. Modern methods allow tracking electronic transactions, analysing communication metadata, and examining digital fingerprints of devices. Advanced machine learning technologies are used to identify hidden connections and anomalies in digital data. Documenting digital crime requires special attention to ensure the legal significance of electronic evidence. Law enforcement agencies use specialised hardware and software systems to create forensic copies of digital data. An important aspect is ensuring the integrity of the evidence base through the use of hashing and electronic signature technologies. An analysis of Kazakhstan's cybersecurity capabilities according to international metrics provides important context for understanding the operative-search environment for combating digital organised crime. According to the National Cyber Security Index (NCSI, 2025), Kazakhstan currently ranks 27th globally with a score of 70.83, demonstrating a moderately strong position in the international cybersecurity landscape. This ranking places Kazakhstan higher in cybersecurity development than its positions in related indices: 48th in the Global Cybersecurity Index, 61st in the Network Readiness Index, while showing stronger performance in E-Government Development (24th globally).

Analysis of specific cybersecurity indicators reveals both strengths and vulnerabilities that directly impact operative-search capabilities. Kazakhstan demonstrates exemplary development in several critical areas, achieving 100% fulfillment in Cybersecurity of Critical Information Infrastructure and Protection of Personal Data. However, the country shows significant room for improvement in Cyber Crisis Management (44% fulfillment) and Cybersecurity Research and Development (50% fulfillment). Of particular relevance to operative-search activities is the Fight Against Cybercrime indicator, where Kazakhstan achieves 69% fulfillment (11 points out of a possible 16), indicating substantial but incomplete development of legal frameworks and technical capabilities for investigating digital crimes (NCSI, 2025).

This data corresponds with the identified challenges in Kazakhstan's operative-search legislation. While the country has established foundational cybersecurity capabilities, gaps remain in specialised approaches to digital evidence collection and processing. The relatively lower scores in research and development suggest limitations in technical capabilities for advanced digital forensics, while the moderate score in fighting cybercrime aligns with the documented challenges in adapting traditional operative-search methods to the

digital environment. These metrics provide objective confirmation of the need for legislative and methodological improvements in Kazakhstan's operative-search activities related to digital organised crime.

International cooperation has become a critical element in the fight against digital crime. Law enforcement agencies from different countries create joint task forces, exchange information in real time and coordinate cross-border operations (KOSHKINBAEVA et al., 2019). Statistics show that about 47% of solved cybercrime is the result of international cooperation (LEUKFELDT and HOLT, 2020). The technical component of digital crime detection includes the use of in-depth network traffic analysis systems. This allows detecting suspicious connections, atypical data transmission patterns, and potential information leakage channels. Special attention is paid to analysing encrypted traffic and identifying hidden communication channels used by criminal groups. The documentation process also involves a detailed recording of the technical profile of the criminal group. This includes analysing the hardware, software, and network infrastructure used. This approach allows not only to collect evidence, but also to predict possible directions of further criminal activity.

Documenting the activities of organised criminal groups in the digital space requires a comprehensive approach to collecting electronic evidence. This includes recording Internet Protocol (IP) addresses, and Media Access Control (MAC) addresses of devices, log files (event log files) of servers and network equipment. Special attention is paid to documenting cryptocurrency transactions, which are often used to finance criminal activities. Special tools are used to analyse blockchain transactions and track the movement of digital assets. Analysis of social media and messengers plays an important role in detecting and documenting digital crimes. Operational units use special techniques to monitor communications between members of criminal groups, identify their connections and hierarchical structure. Special attention is paid to documenting the use of anonymisation and encryption technologies by criminals. In the section on methods for detecting and documenting digital crimes, an analysis of statistics from the Committee on Legal Statistics of the Republic of Kazakhstan (2023) showed that specialised cybercrime units have begun to actively implement the latest digital forensics methods (SANIYAZOVA et al., 2024). In 2023, 21,358 cybercrimes were registered, with the share of crimes committed by organised groups at 17% (Organisation for Security and Co-operation in Europe (OSCE), 2024). The study showed that a comprehensive approach to detecting digital crimes, including monitoring of network activity, was the most effective, which allowed detecting 42% of all recorded offences (BOLATBEK et al., 2024). The analysis of financial transactions and digital traces has demonstrated significant efficiency, which has led to the detection of 27% of criminal activity

(ZHAMIYEVA and ALBEKOVA, 2023). According to research, prompt introduction into the digital environment allowed solving 18% of crimes, and work with informants in the Information Technology (IT) sector contributed to the detection of 13% of cases of illegal activity (SHAISULTANOV et al., 2024).

To effectively document digital crime, methods of visualising digital evidence are used. This includes the creation of timelines of events, diagrams of relationships between members of criminal groups, and maps of the infrastructure used. This approach allows for a clear presentation of complex technical evidence and facilitates its perception during further investigation.

An analysis of legal regulation and practical methods of combating digital organised crime in different countries has revealed significant differences in approaches and the level of technological support. As shown in Table 1, the Republic of Kazakhstan demonstrates a consistent development of the legal framework and institutional structure, introducing modern methods of detecting and documenting digital crime.

Characteristic	**Republic of Kazakhstan**	**Organisation for Economic Co-operation and Development (OECD) countries**	**Commonwealth of Independent States (CIS) countries**
Regulatory and legal framework	Law "On Operational and Investigative Activities"	Comprehensive cybersecurity legislation, specialised acts on digital evidence	Basic legislation on Operational and Search Activities (OSA) with elements of digital sphere regulation
Institutional structure	Specialised units in law enforcement agencies	Separate cybersecurity agencies, specialised courts	Units within traditional law enforcement agencies
Technical support	Modern monitoring and data analysis systems	Advanced AI and machine learning technologies	Basic monitoring systems
International cooperation	Active participation in regional initiatives	A developed system of international interaction	Limited cooperation within the CIS

Documentation features	Standardised protocols, electronic evidence	Automated systems, blockchain technologies	Traditional documentation methods

Table 1 – Comparative analysis of legal regulation and methods of combating digital organised crime.

Source: compiled by the authors based on Law of the Republic of Kazakhstan No. 54-XIII "On Operational and Investigative Activities" (1994), Criminal Procedure Code of the Republic of Kazakhstan (2014), S. Shaisultanov et al. (2024).

Comparative analysis has shown that OECD countries have the most developed system of countering cybercrime, including specialised agencies and advanced technological solutions. At the same time, the experience of countries with positive practices of implementing innovative methods of documentation, including the use of blockchain technology and AI to analyse digital evidence, attracts special attention (GARCIA and BROWN, 2022).

An important aspect is to ensure that digital crimes are documented promptly. The speed of response to the detected facts of criminal activity often determines the possibility of preserving digital evidence. To this end, automated monitoring and response systems are being developed and implemented to promptly record signs of illegal activity.

In the context of international cooperation, special attention is paid to the standardisation of procedures for documenting digital crimes. This includes the use of unified protocols for recording digital evidence, ensuring its admissibility in different jurisdictions, and creating secure channels for information exchange between law enforcement agencies of different countries.

Tactical Peculiarities of Conducting Operational and Investigative Measures

In the context of the digital transformation of society, the tactics of conducting operational and investigative activities are undergoing significant changes. Modern organised criminal groups are actively using digital technologies, which requires the development and implementation of new tactical approaches to their detection and documentation. According to Article 11 of the Law of the Republic of Kazakhstan "On Operational and Investigative Activities" (1994), operational units are authorised to use a wide range of operational and investigative measures, including surveillance in telecommunication networks, control of messages, operational implementation into criminal groups, and covert acquisition of information. However, the rapid development of digital technologies creates new challenges in applying these measures to cybercrimes, which are not fully addressed in the current legislation. In the area of tactical

features of conducting operational search activities, the analysis revealed a significant increase in efficiency when using an integrated approach (AKHMETOV and RYSMAGAMBETOVA, 2022). The greatest effectiveness was demonstrated by the joint use of technical means and agent work, which ensured the success of solving crimes in 76% of cases (ALIMKULOV et al., 2023).

Multi-level monitoring of digital activity was effective in 68% of cases, and the use of digital intelligence methods led to positive results in 62% of cases (SEITZHANULY et al., 2022). According to the official statistics of the Committee on Legal Statistics of the Republic of Kazakhstan (2023), law enforcement agencies registered 21,358 cybercrimes, with a clearance rate of 43%. This relatively low clearance rate highlights the need for improving tactical approaches to investigating digital crimes. According to current data, investigation times varied depending on the type of crime: detecting and documenting financial fraud took an average of 2.3 months, crimes against information security – 3.7 months, and e-commerce crimes – 1.8 months (KAIYRBEKOVA, 2024).

The theoretical analysis of the essence of operational and investigative measures in the digital environment allows us to identify their key features. Firstly, it is the need to combine traditional methods of operational work with the use of special technical means for monitoring the digital space. Second, an important characteristic is the increased requirements for secrecy in the context of digital transparency. Thirdly, the speed of response to detected facts of criminal activity is of particular importance due to the high dynamism of the digital environment.

The practice of conducting operational and investigative activities shows that effective counteraction to digital organised crime requires the integrated use of various tactical techniques. A special role is played by the prompt introduction of criminal groups into the digital environment. This requires the creation of credible digital legends that include not only documentary cover, but also a plausible digital history and network activity.

According to Law of the Republic of Kazakhstan "On Operational and Investigative Activities" (1994), operational implementation is one of the most complex operational measures requiring comprehensive preparation. In the digital environment, this measure faces additional challenges related to the virtual nature of communication and the high technical literacy of cybercriminals. The Department for Combating Cybercrime, established within the Ministry of Internal Affairs on November 4, 2024, has implemented specialised protocols for digital infiltration operations that take into account these complexities (Adyrna.kz, 2024).

An important tactical element is the organisation of covert surveillance in the digital space. This includes monitoring social media, messengers, and other communication channels used by criminal groups. It is necessary to consider the ability of criminals to detect the fact of surveillance through the analysis of digital traces.

Under Article 12 of the Law "On Operational and Investigative Activities" (1994), law enforcement agencies are authorised to conduct covert surveillance, including in digital networks. However, the law lacks specific provisions on monitoring encrypted communications and anonymised networks (such as TOR, VPN services), which are commonly used by organised criminal groups. This legislative gap significantly limits the effectiveness of surveillance measures in the digital environment.

Special attention should be paid to the tactics of conducting operational combinations in the digital environment. It should take into account the ability of criminals to quickly change communication channels, use encryption and anonymisation methods, and the availability of criminal groups' own security systems. An important element is the coordination of the actions of various units involved in the operational combination, considering the technical features of the digital environment.

In the context of international cooperation, the tactics of joint operational activities are of particular importance (AIDARBAYEV and UDERBAYEVA, 2020a; SHAKEEVA et al., 2025). This requires coordination not only of legal aspects but also of the technical capabilities of various law enforcement agencies, ensuring compatibility of the technical means and methods used to document criminal activity.

The Republic of Kazakhstan has signed multilateral agreements within the framework of the SCO and the CIS on cooperation in combating cybercrime. These agreements provide legal mechanisms for joint operational activities, but their implementation is complicated by technical incompatibilities and procedural differences. The Resolution of the Government of the Republic of Kazakhstan "On Approval of the Cybersecurity Concept "Cybershield of Kazakhstan" (2017) identifies international cooperation as a priority area but does not provide specific mechanisms for tactical coordination in joint operations.

Empirical research shows that the current practice of conducting operational and investigative activities in the digital environment faces a number of specific challenges. Of particular importance is the issue of ensuring the admissibility of collected digital evidence. The concept of "electronic evidence" is not explicitly defined in the Criminal Procedure Code of the Republic of Kazakhstan (2024), which creates significant problems in establishing its authenticity and admissibility in court. Article 111 of the Criminal Procedure

Code (2014) defines types of evidence broadly, but lacks specific provisions for digital evidence. In practice, this leads to situations where valuable digital information cannot be properly introduced as evidence. Practice shows that operational units need to thoroughly document each stage of obtaining digital data, ensuring the possibility of further verification of its authenticity and integrity.

For example, consider a specific case from the practice of law enforcement agencies in Kazakhstan. In 2023, during the investigation of an organised criminal group that specialised in fraud using phishing websites, it was necessary to document digital evidence of their criminal activities (SHAISULTANOV et al., 2024). At the first stage, the operatives discovered a phishing site that imitated a banking service portal, which constitutes a violation of cybersecurity legislation. To document this fact, a forensic copy of the web page was created using specialised software in accordance with established procedures (Cybersecurity Act, 2023). Not only the visual elements of the website were recorded, but also its programme code, metadata and hosting information. Each action was documented in a special protocol, indicating the exact time, technical means used, and responsible persons. The next step was to track financial transactions related to criminal activity. For this purpose, special analytical tools were used to visualise the movement of funds and establish relationships between different bank accounts. All identified transactions were documented with the creation of secure copies of bank statements and transaction logs. Particular attention was paid to preserving the integrity of digital evidence. A Secure Hash Algorithm 256-bit (SHA-256) checksum was created for each file, which allowed us to further confirm that the data had not been altered (Cybersecurity Act, 2023). All information was stored on specially protected media with limited access and a system for logging all operations. Thanks to this thorough approach to documentation, all the collected digital evidence was recognised as admissible in court, which allowed successfully proving the guilt of the members of the criminal group.

Despite this successful case, many operational units face significant difficulties in documenting digital evidence due to the lack of standardised procedures and clear legal guidelines. The Normative Resolution of the Supreme Court of the Republic of Kazakhstan "On Amendments and Supplements to Certain Regulatory Resolutions of the Supreme Court of the Republic of Kazakhstan on Criminal and Criminal Procedure Legislation" (2018) attempted to address this issue, but its provisions remain too general to provide practical guidance for complex digital investigations.

The analysis of practical experience shows that the effectiveness of operational and investigative measures largely depends on the correct choice of

the moment of their implementation. In the digital environment, this aspect is of particular importance due to the possibility of rapid destruction of electronic evidence. The tactic of simultaneously conducting a set of operational and investigative measures in different geographical locations requires precise synchronisation of actions and reliable communication channels between units.

The practice of combating digital organised crime demonstrates the need to constantly adapt tactical techniques to new technological capabilities of criminals. It is particularly difficult to identify and document the activities of criminal groups that use decentralised management and communication systems. In such cases, traditional methods of infiltration and surveillance need to be significantly modified to take into account the peculiarities of the digital space.

An important aspect is the tactics of conducting operational and technical measures in the digital environment. Practice shows that the success of such measures depends on the correct choice of technical means, their timely updating and adaptation to new methods of encryption and information protection used by criminal groups. At the same time, special attention should be paid to ensuring the secrecy of technical means and methods of their use.

The Department for Combating Cybercrime of the Ministry of Internal Affairs has recently implemented advanced technical solutions for digital investigations, including AI-based systems for analysing digital traces and specialised software for decrypting protected communications. However, the legal basis for using these tools remains underdeveloped. Articles 13 and 14 of the Law "On Operational and Investigative Activities" (1994) provide general provisions on the use of technical means but do not address the specifics of modern digital forensics tools.

The comprehensive analysis of Kazakhstan's legislative framework governing operational and investigative activities reveals several significant gaps that impede effective counteraction to digital organised crime. The Law of the Republic of Kazakhstan "On Operational and Investigative Activities" (1994), despite multiple amendments, still lacks specific provisions addressing the unique challenges of digital investigations. For instance, Article 11, which enumerates permissible operational measures, does not adequately address methodologies for collecting and preserving volatile digital evidence.

The analysis of specific operational and investigative activities practices in Kazakhstan demonstrates that operational units often resort to using general provisions of the law to justify specialised digital investigation techniques. For example, network traffic interception is conducted under the broader category of "control of messages" (Article 11, paragraph 7), without specific guidelines addressing the technical and legal nuances of packet capture and analysis. This

regulatory ambiguity forces operational officers to navigate a grey area of legal interpretation, potentially compromising the admissibility of collected evidence.

Case studies from the Almaty and Astana cybercrime units further reveal practical challenges in implementing Article 14's provisions on the technical means of usage. In multiple instances, advanced digital forensics tools were employed without clear procedural guidelines, resulting in challenges to evidence authenticity at later trial stages. The recent implementation of SHA-256 verification protocols for digital evidence by the Ministry of Internal Affairs represents an ad hoc solution to a problem that requires comprehensive legislative attention.

The experience of international cooperation in combating digital organised crime demonstrates the need to develop common tactical approaches and standards for conducting investigative activities. This is especially important in cross-border operations, where success depends on the coordination of actions of law enforcement agencies from different countries and their ability to promptly exchange information on the detected facts of criminal activity.

International Cooperation in Combating Transnational Cybercrime

The scientific and legal analysis of international cooperation in combating transnational cybercrime reveals an extremely complex and dynamic system of global legal interaction which is constantly transforming under the influence of technological and social changes. The evolution of international legal mechanisms for combating cybercrime has deep historical and technological roots. The Budapest Convention on Cybercrime (2001) was the first fundamental document that launched an international approach to understanding cyberspace as a single global environment requiring unified legal mechanisms for regulation. The UN Convention against Transnational Organised Crime (2004) fundamentally changed the paradigm of perception of criminal groups, defining them not as local but as global network structures. Research by M. Chertoff and D.S. Reddy (2022) convincingly proves that modern cybercrime groups are complex self-organised systems that can instantly adapt to changes in the legal field.

The technological evolution of cybercrime is outpacing the pace of legal regulation (APAKHAYEV et al., 2018; ALIKHANOV and BUSURMANKULOVA, 2022). Criminal networks are transforming into highly intelligent adaptive systems that use the latest encryption, anonymisation and decentralised management technologies. AI and blockchain technologies are becoming not just tools, but fundamentally new environments for criminal activity. A report by the European Union Agency for Cybersecurity (ENISA, 2023) documents a fundamental change in the nature of cyber threats. Whereas

earlier single hacker attacks dominated, today we are dealing with highly organised transnational criminal ecosystems that have their own economy, social structure and communication systems.

A comparative analysis of the legislation of different countries reveals radical differences in approaches to regulating cyberspace. The Estonian Cybersecurity Act (2023) demonstrates a model of total digitalisation of the law enforcement system, the Singapore Cybersecurity Act (2018) focuses on preventive mechanisms, while the legislation of post-Soviet states, in particular Kazakhstan, chooses an eclectic approach of combining administrative and technological tools. The study by E. Garcia and T. Brown (2022) shows revolutionary changes in the methods of investigating cybercrime. Traditional investigative actions are giving way to high-tech analytics using machine learning, which can process huge amounts of distributed data and identify hidden patterns of criminal activity.

The OECD Guidelines on Digital Security Risk Management (2025) actually form a new area of international law – digital jurisprudence, based on the principles of prevention, transparency and global cooperation. The key goal is not to punish, but to prevent and neutralise potential cyber threats. E.R. Leukfeldt and T.J. Holt demonstrate in their work the formation of fundamentally new social structures, where geographical boundaries, nationality and traditional hierarchies lose all meaning. Horizontal networks based on technological competences and common economic interests come to the fore.

The practice of international investigations of S. Shaisultanov et al. (2024) reveals critical transformations in the system of international legal interaction. The classic mechanisms of extradition, mutual legal assistance and interstate cooperation are giving way to flexible expert networks that can respond quickly to the challenges of the digital environment.

Transnational cybercrime as a global security challenge of our time is a complex, multidimensional system of illegal activity that is constantly evolving under the influence of technological transformations (SEMENENKO et al., 2021a; AIDARBAYEV and UDERBAYEVA, 2020b). Modern cybercriminal groups demonstrate a high level of adaptability, technological sophistication and the ability to quickly reconfigure their network structures.

Understanding the dynamics of changes in the mechanisms of countering cybercrime requires a comprehensive approach that takes into account the technological, legal, social and psychological aspects of this phenomenon. That is why, in the context of the study, a comparative table was developed (Table 2), which demonstrates the evolutionary trajectory of international mechanisms for combating transnational cybercrime.

Comparison criterion	Traditional approach	Modern approach	Promising transformations
Jurisdictional boundaries	Clearly defined state borders	Blurred cross-border spaces	Formation of virtual legal ecosystems
Technological tools	Static investigation methods	Dynamic AI systems	Quantum and neural network technologies
Communicative models	Hierarchical departmental communications	Horizontal expert networks	Self-organised global platforms
Sources of information	Official databases	Distributed information environments	Predictive analytics systems
Subjects of resistance	State law enforcement agencies	Interstate and private structures	Global cyberpolice communities
Preventive mechanisms	Reactive response	Proactive monitoring	Predictive risk management
Financial instruments	Traditional banking systems	Cryptocurrency and blockchain technologies	Decentralised financial ecosystems
Educational strategies	Highly specialised training	Interdisciplinary competencies	Adaptive learning trajectories

Table 2 – Comparative analysis of international mechanisms for combating transnational cybercrime.

Source: compiled by the authors based on Budapest Convention on Cybercrime (2001), Law of the Republic of Kazakhstan No. 418-V "On Informatisation" (2015), Cybersecurity Act (2018).

The table reveals the key transformation processes by comparing traditional and modern approaches based on such criteria as jurisdictional boundaries, technological tools, communication models, information sources, counteraction actors, preventive mechanisms, financial instruments and educational strategies. The presented model allows not only to record the current state of international cooperation in the field of combating cybercrime, but also to outline promising areas for its further evolution.

The development of information and communication technologies and the global digitalisation of social processes create fundamentally new challenges in

the field of international security, especially in relation to combating transnational cybercrime (SMAILOV et al., 2025b; SEMENENKO et al., 2021b). A comprehensive analysis of the regulatory framework of the Republic of Kazakhstan and international legal documents allows us to formulate the key areas of interstate cooperation in countering cyber threats.

The international legal context for combating transnational cybercrime is formed by a number of fundamental international conventions that create a unified platform for the interaction of law enforcement agencies of different states. In particular, the Budapest Convention on Cybercrime (2001) was the first international treaty aimed at unifying approaches to criminal liability in cyberspace. The Council of Europe Convention on Laundering (2005) further strengthened the mechanisms of international cooperation in combating economic crimes in the digital environment.

Of particular importance is the UN Convention against Transnational Organised Crime (2004), which created a comprehensive international legal framework for state cooperation in combating organised crime, including its cyber component. In the field of international cooperation in combating transnational cybercrime, statistics showed that in 2023, 47% of all detected organised cybercrime was transnational in nature (ZHAKENOV et al., 2024). An analysis of the dynamics of international cooperation showed a significant increase: the number of joint operations with law enforcement agencies of other countries increased by 156% compared to 2019 (KASSYMZHANOVA et al., 2022). The response time to international requests decreased from 45 to 12 days, and the overall efficiency of international cooperation increased by 78% (SULTANBAYEVA et al., 2023). The most active cooperation was with law enforcement agencies of the European Union, which accounted for 34% of joint operations, Central Asia – 29%, Southeast Asia – 22%, and other regions – 15% (OSCE, 2024). Statistics indicate a higher success rate in investigating cases with an international element, with a successful completion rate of 72%, which is significantly higher than the 43% for local cybercrime (ZHAKUPOV, 2024). This data confirms the growing importance of international cooperation in combating digital organised crime and the need to further improve cooperation mechanisms (KHAMZIN et al., 2023).

A comparative analysis of foreign legislative acts reveals a tendency towards unification of approaches in the field of cybersecurity. The Singapore Cybersecurity Act (2018), the Estonia Cybersecurity Act (2023) and the Law of the Republic of Uzbekistan "On Operational Investigative Activities" (2012) demonstrate common principles and mechanisms for countering cyber threats. Countries are increasingly realising that isolated national cybersecurity models are unable to effectively counteract complex forms of transnational cybercrime.

Therefore, the key drivers of unification are: first, the harmonisation of international legislation; second, the unification of technological standards for information security; and third, the creation of mechanisms for prompt interstate information exchange and coordination of law enforcement actions. Singapore demonstrates an advanced model of technological regulation, Estonia presents a highly effective digital security system, and Uzbekistan adapts international best practices to its own legal context, which confirms the thesis of convergence of approaches in the field of cybersecurity.

Based on the results of the study, specific recommendations can be offered for improving legal regulation and practical activities in the field of combating cybercrime. Analysis of Chapter 15 of the Criminal Procedure Code of the Republic of Kazakhstan (2014) reveals several gaps in the regulation of electronic evidence. While Article 111 defines types of evidence broadly, it lacks specific provisions addressing the unique characteristics of digital evidence. Article 126, which regulates the use of scientific and technical means in the process of proof, provides only general guidelines insufficient for the complexities of digital forensics. Specifically, the Criminal Procedure Code should be amended to include new provisions in Chapter 15 that establish clear criteria for the authenticity and integrity of digital evidence, including hash verification protocols and chain of custody documentation specific to electronic data. These amendments should define procedures for preserving volatile digital evidence that may be lost during traditional evidence collection processes and establish standards for metadata preservation and analysis as a component of digital evidence.

Currently, Article 126 permits the use of scientific and technical means for evidence collection but lacks detailed procedures for digital environments. This creates practical challenges for investigators, as evidenced in recent cases where digital evidence was contested due to procedural ambiguities. For example, in cases involving cryptocurrency transactions, courts have struggled with applying traditional evidentiary standards to blockchain data.

Regarding operational and investigative activities, the Law "On Operational and Investigative Activities" (1994) requires modernisation to address digital environment specifics. While this law provides a legal basis for traditional investigative techniques, it inadequately addresses digital space operations. The law should be supplemented with provisions that define specialised investigative techniques for digital environments, including procedures for darknet monitoring that comply with privacy protections. These provisions should establish legal frameworks for cryptocurrency transaction monitoring, addressing the technical and jurisdictional challenges unique to digital assets, and set clear boundaries and oversight mechanisms for the use of

AI in data analysis. These legislative gaps have created practical challenges documented in recent investigations, where ambiguities in legal procedures have complicated prosecution efforts against transnational cybercriminal groups.

The organisational infrastructure for combating cybercrime has seen positive developments with the creation of the Department for Combating Cybercrime within the Ministry of Internal Affairs in November 2024. This initiative addresses the organisational recommendations identified in the research. The focus should now shift to enhancing the capabilities of this department through developing specialised training programs on advanced digital forensics techniques and establishing collaboration frameworks with academic and private sector cybersecurity experts. The technological modernisation efforts of law enforcement agencies have progressed significantly, particularly in the area of financial monitoring systems used to combat terrorism financing and financial pyramids. These systems, governed by departmental regulatory acts, provide a foundation for broader technological initiatives. Building on these existing systems, further development should focus on integration capabilities that allow for coordinated data analysis across agencies while maintaining appropriate privacy and security protocols.

The analysis of Kazakhstan's legislative framework governing electronic evidence reveals significant gaps that impede effective counteraction to digital organised crime. While Article 111 broadly defines types of evidence, it lacks specific provisions addressing the unique characteristics of digital evidence. Similarly, Article 126, which regulates the use of scientific and technical means in the evidentiary process, provides only general guidelines insufficient for the complexities of digital forensics.

In Kazakhstan's legislation, there is no clear definition of "electronic evidence". In practice, electronic evidence is understood as digital data that can be used to establish the circumstances of a case and has significance for its proper resolution. This includes files, metadata, event logs, electronic transactions, social media information, messenger correspondence, data from electronic media, and other digital artifacts.

The legal regulation of electronic evidence in Kazakhstan is currently implemented through several normative acts. The Criminal Procedure Code of the Republic of Kazakhstan (2014) serves as the primary document regulating evidential matters, but its provisions regarding digital evidence are insufficient. The Law "On Operational and Investigative Activities" (1994) defines general frameworks for conducting operational measures but is inadequately adapted to the digital environment. Additional regulation comes from Normative Resolutions "On Amendments and Supplements to Certain Regulatory Resolutions of the Supreme Court of the Republic of Kazakhstan on Criminal and

Criminal Procedure Legislation" (2018) and "On Certain Issues of Sanctioning Preventive Measures" (2020).

Kazakhstan has already established certain mechanisms for working with electronic evidence. The Department for Combating Cybercrime was created within the Ministry of Internal Affairs structure in 2023. Modern technologies for monitoring and analysing data have been implemented, along with methods for documenting digital traces. International cooperation has been established within regional initiatives such as the SCO and the CSTO. Financial monitoring systems are operating to counter terrorism and financial pyramids.

However, the incomplete legal regulation of electronic evidence leads to numerous problems. Legal uncertainty when working with digital traces arises from the absence of clear criteria for the admissibility and reliability of electronic evidence. There are difficulties in establishing the authenticity of electronic evidence due to the lack of standardised procedures. Problems with maintaining the integrity of digital data persist, as there are no clear protocols to ensure information remains unchanged. Difficulties arise when working with volatile data that may be lost when traditional evidence collection methods are used. Courts experience challenges when evaluating digital evidence, especially in complex cases involving cryptocurrencies and blockchain technologies. Additionally, there is insufficient regulation of encrypted communications monitoring and anonymised networks like TOR and VPN services.

Amendments to the Criminal Procedure Code (2014) are necessary for several reasons. The Code is the main normative act regulating evidential matters, and including appropriate norms will ensure uniformity in law enforcement practice. Clear regulation in the Code will create legal guarantees for the admissibility of electronic evidence. Including provisions on electronic evidence in the Criminal Procedure Code will allow their integration into the general system of evidentiary law and provide participants in the process with the opportunity to challenge violations of procedures for collecting and examining electronic evidence.

To improve the legal regulation of electronic evidence, several legislative changes are proposed. The Criminal Procedure Code should include a definition of "electronic evidence". Criteria for the admissibility and reliability of electronic evidence must be established. Procedures for collecting and storing digital data while ensuring their integrity need to be developed. The procedure for conducting digital forensic examination should be defined. Rules for using modern technologies such as AI and machine learning for analysing digital traces must be established. The procedure for international cooperation in investigating transnational cybercrimes should be regulated. Mechanisms for judicial control

over operational and investigative activities in the digital environment need to be created.

Specifically, the Criminal Procedure Code should be amended to include new provisions in Chapter 15 that establish clear criteria for the authenticity and integrity of digital evidence, including hash verification protocols and chain of custody documentation specific to electronic data. These amendments should define procedures for preserving volatile digital evidence that may be lost during traditional evidence collection processes and establish standards for metadata preservation and analysis as a component of digital evidence.

In conclusion, a comprehensive modernisation of Kazakhstan's legislation regarding electronic evidence regulation is necessary for effective counteraction to digital organised crime. This modernisation should include amendments to the Criminal Procedure Code, the Law "On Operational and Investigative Activities", and the development of consistent departmental regulations that provide clear guidelines for law enforcement agencies working with electronic evidence

Special attention should be paid to ensuring technical capabilities for cryptographic examination and analysis of complex digital evidence. In the area of preventive activities, it is recommended to develop and implement a system for the early detection of cyber threats based on machine learning technologies. Such a system should ensure the ability to respond promptly to new types of cybercrime and include mechanisms for cooperation with the private sector in the field of cybersecurity. An important element of prevention is the creation of an effective system for exchanging information on cyber threats in real time. Particular attention should be paid to the development of international cooperation in combating cybercrime. At the legal level, it is necessary to ensure the harmonisation of national legislation with international standards and create effective mechanisms for joint international investigations. The practical aspect of cooperation should include the creation of channels for the rapid exchange of information between countries, the organisation of regular international exercises and the development of protocols for joint response to cyber incidents.

Implementation of the proposed recommendations will significantly increase the effectiveness of combating cybercrime, provide law enforcement agencies with the necessary legal and technical tools to detect, document and investigate digital crimes, and create a solid basis for international cooperation in this area. A comprehensive approach to the modernisation of the cybercrime system, including legislative improvements, organisational changes and technological development, will allow for an adequate response to the current challenges of digital crime.

DISCUSSION

The study represents a comprehensive approach to the study of operational and investigative activities in the context of digital transformation of crime. The scientific significance of the study lies in the systematic analysis of the evolution of mechanisms for combating transnational cybercrime, which is becoming increasingly complex and sophisticated in the globalised information space.

The current scientific discourse on combating cybercrime demonstrates the evolution from a technocratic to a more integrated understanding of the problem. A striking example of such a comprehensive approach is the study by M. Chertoff and D.S. Reddy (2022), who went beyond a purely technical analysis of cyber investigations. Their work reveals the multilevel nature of cross-border investigations, where technological barriers are inextricably intertwined with legal challenges and institutional constraints.

A revolutionary look at the social architecture of cybercrime was presented by E.R. Leukfeldt and T.J. Holt (2020), revealing the dynamic nature of criminal communities in digital space. Of particular value is the identification of complex relationships between the virtual and real activities of criminal groups. This methodological breakthrough allows us to rethink traditional approaches to operational and investigative activities. In the context of the technological transformation of law enforcement, it is worth paying attention to the practical recommendations of W. Van der Wagen and W. Pieters (2020). Their concept of the "hybrid victim" opens up new perspectives for understanding the mechanisms of victimisation in the digital space. Their approach allows for the integration of technological and social aspects of cybercrime into a single analytical framework. A fundamentally new direction in the study of cybercrime is opened by E. Garcia and T. Brown (2022). The authors propose to reconsider the role of AI in the investigation of digital crimes, considering it not just as a tool but as an integral element of the modern law enforcement system. Their conclusions significantly expand the methodological arsenal of operational and investigative activities in the digital space.

The transformation of cybercrime requires a deep rethinking of approaches to its study. The behavioural dimension of this problem is skilfully revealed in the work of G. Sarkar and S.K. Shukla (2023). Their system of behavioural profiling of cybercriminals goes beyond traditional forensic methodology by integrating psychological, social and technological aspects into a single analytical framework. Their contribution to understanding latent forms of criminal activity is particularly valuable, opening up new opportunities for operational and investigative activities.

In parallel, the sociological understanding of digital crime is developing. A. Di Nicola (2022) convincingly demonstrates how digitalisation is radically changing the very nature of organised crime. At the intersection of sociology, criminology, and technology studies, the author provides a new theoretical framework for understanding contemporary criminal communities. This study does not simply complement existing theories, but offers a fundamentally new paradigm for analysing criminal structures in the digital age.

The technological breakthrough in the field of countering cybercrime is reflected in the study by E. Garcia and T. Brown (2022). Instead of the traditional view of AI as an auxiliary tool, the authors propose to consider it as an integral part of the modern law enforcement system. Their methodology for integrating machine learning into investigative activities demonstrates how technological innovations can radically improve the efficiency of detecting and documenting cybercrime.

The study by K.K.R. Choo (2008) on the typology of organised criminal groups in cyberspace is fundamental to understanding the evolutionary processes of cybercrime. The author proposed a unique classification model that reveals the internal structure and mechanisms of functioning of cybercrime groups long before large-scale digitalisation. The presented research proves that the conceptual provisions of K.K.R. Choo's study were ahead of their time and remain relevant even a decade and a half after its publication. The author's thesis on the transformational potential of cyberspace as an environment that fundamentally changes the logic of organising criminal activity deserves special attention. The typology developed by the researcher demonstrates the complex internal architectonics of cybercrime groups, their ability to quickly adapt and reconfigure in the face of constant technological change.

The scientific study by T.J. Holt et al. (2020), devoted to the research of challenges in the investigation of online crimes related to the exploitation of minors, represents an extremely important area of criminological research. The authors have carried out a comprehensive analysis of methodological and practical problems that arise during the investigation of particularly dangerous categories of cybercrime. The presented research demonstrates the fundamental complexity of documenting crimes in the digital environment, especially when it comes to latent forms of illegal activity. The study by T.J. Holt et al. reveals the systemic methodological challenges faced by law enforcement agencies in the process of detecting and suppressing cybercrime involving the most vulnerable categories of the population. The authors' conclusion about the need to develop specialised investigative techniques that take into account the technological specifics of the modern digital environment is of fundamental importance.

The study by C. Horan and H. Saiedian (2021), dedicated to the landscape of cyber investigations, presents an extremely important scientific study that reveals the complex issues of combating cybercrime. The authors have carried out a fundamental analysis of current challenges and prospects for the development of methodological approaches to cyber investigations. The fundamental significance of the presented work lies in the comprehensive approach to the study of evolutionary transformations of mechanisms for combating cybercrime. The study by C. Horan and H. Saiedian demonstrates that traditional law enforcement methodologies are exhausting their potential in the context of total digitalisation and require radical modernisation.

The global COVID-19 pandemic has created a unique opportunity to study how large-scale crises affect the evolution of cybercrime. S. Kemp et al. (2021) conducted a pioneering study using time-series analysis to track changes in criminal activity during the crisis period. Their methodological approach allowed them not only to capture changes in cybercrime patterns, but also to identify causal links between crisis events and the transformation of criminal activity.

Deepening this understanding, H.S. Lallie et al. (2021) and M. Bitaab et al. (2021) expanded the scope of the analysis by focusing on the specific mechanisms by which criminal groups adapt to new realities. These studies identified three key trends in the crisis period: intensification of attacks on critical infrastructure, exponential growth of phishing campaigns, and a significant expansion of activity in the darknet space. Particularly important is the conclusion that crisis conditions not only change the tactics of criminals but also accelerate the technological evolution of criminal practices.

In the context of the study of legal mechanisms for combating cybercrime, the work of E.V. Mitskaya and G.S. Shkabin (2021), who studied an important aspect of operational and investigative activities – the legal regulation of lawful infliction of harm during covert actions by law enforcement agencies. Their analysis of the legislative experience of the Republic of Kazakhstan reveals a complex dialectic between the need for effective operational and investigative measures and ensuring the legality of their implementation. The authors pay special attention to the fact that in the context of digital transformation of crime, there is a need to rethink traditional approaches to the regulation of covert work. Their conclusions regarding the need to improve the legal regulation of operational and investigative activities are of particular relevance in the context of combating new forms of digital organised crime, where complex operational combinations in the virtual space are often required.

The synthesis of these studies forms a new perspective on the relationship between social crises and cybercrime. Whereas previously crises were seen mainly as catalysts for traditional crime, current analysis demonstrates their role

in shaping fundamentally new forms of criminal activity in the digital space. This understanding requires a fundamental rethinking of approaches to cybersecurity, especially in the context of preparedness for future global challenges.

The institutional capacity of law enforcement agencies is becoming a key factor in successfully countering modern forms of crime. An in-depth analysis of this issue is presented in the study by O.M. Omelchuk et al. (2022), who consider the law enforcement system as a complex organisational mechanism where the effectiveness of crime counteraction depends on the coordinated work of all components. Their work is particularly valuable for identifying critical points in the system of interagency cooperation. The researchers identified three fundamental problems that significantly reduce the effectiveness of law enforcement. The first is information barriers between different agencies, which create a kind of "blind spot" in the crime fighting system. The second problem is the lack of unified standards for the exchange of operational data, which leads to the loss of important information at the interagency level. The third challenge is related to the imperfection of the regulatory framework, which often fails to keep pace with the evolution of criminal practices. The significance of this study goes beyond the mere diagnosis of problems – it lays a methodological foundation for the systemic modernisation of law enforcement structures. Understanding the relationship between information interaction, standardisation of procedures and legal regulation allows us to develop a comprehensive approach to improving the effectiveness of combating organised crime in its modern forms.

The scientific work of R.M. Zhamiyeva et al. (2022) reveals an important issue of the role of financial investigations in the fight against money laundering, which is directly related to combating organised crime in the digital space. The authors have carried out a thorough analysis of the methodological and practical aspects of conducting financial investigations in the digital economy.

Thus, the analysis of additional scientific sources demonstrates the multifaceted nature of the problem of combating organised crime in the digital space and emphasises the need for a comprehensive, interdisciplinary approach to its solution. Each of the reviewed studies makes a unique contribution to understanding various aspects of this complex problem, from victimological aspects to institutional mechanisms of counteraction, and together they form a more complete picture of the current state and prospects for the development of operational and investigative activities in the context of digital transformation of crime.

CONCLUSIONS

The study allows us to draw a number of important conclusions regarding operational and investigative activities in the context of countering new forms of digital organised crime. The analysis of the current state and trends in the development of digital crime indicates fundamental changes in the structure and methods of activity of organised criminal groups. Modern criminal organisations demonstrate a high level of technological adaptability, actively using the latest digital tools to improve their illegal activities. This creates fundamentally new challenges for law enforcement agencies, requiring a significant modernisation of operational and investigative methods. The study revealed the formation of complex, multi-level criminal ecosystems in cyberspace. These ecosystems are characterised by a high degree of decentralisation, a flexible structure and the ability to quickly adapt to changes in the environment. The trend towards convergence of different types of cybercrime, when traditional forms of organised crime are integrated with high-tech cybercrime, is particularly dangerous. Such integration significantly complicates the processes of detecting and documenting criminal activity, requiring law enforcement agencies to apply comprehensive, interdisciplinary approaches. The analysis of the legal framework has revealed significant gaps in the regulation of operational and investigative activities in the digital space. The existing legal framework often fails to keep pace with the rapid development of technology and new forms of crime. This creates serious legal conflicts and complicates the process of collecting and using electronic evidence. A comprehensive modernisation of criminal, criminal procedure and investigative legislation is needed, taking into account the specifics of the digital environment and new forms of criminal activity. The study confirmed the critical importance of international cooperation in combating transnational cybercrime.

The global nature of the digital space requires the development of effective mechanisms for the prompt exchange of information and coordination of law enforcement agencies from different countries. Particular attention should be paid to harmonising legislation and procedures for cross-border investigations, as well as creating common standards for the collection and processing of digital evidence. The study highlighted the critical role of technological support for investigative activities. Effective counteraction to digital crime requires constant updating and improvement of special hardware, big data analysis software, tools for monitoring cyberspace and conducting digital forensics. Particular attention should be paid to the development of AI and machine learning systems to automate the processes of detecting and analysing digital traces of criminal activity. An analysis of the practice of documenting digital crimes has revealed the need to develop new methodological approaches to the collection and

processing of electronic evidence. Particular attention should be paid to ensuring the integrity and reliability of digital evidence, developing standardised protocols for its recording and storage. Another important aspect is the development of methods for visualising complex digital evidence for its effective presentation in court. In summary, effective counteraction to new forms of digital organised crime requires a comprehensive, systematic approach that integrates legal, organisational, technological and social aspects. It is necessary to develop a new paradigm of operational and investigative activities that considers the dynamic nature of the digital environment and is able to adapt to constantly evolving forms of crime. This requires not only technological modernisation, but also a conceptual rethinking of the principles and methods of operational work in the global information society.

It is necessary to note certain limitations of this study that should be taken into account when interpreting its results. Firstly, the study focuses mainly on the experience of the Republic of Kazakhstan and a limited number of foreign countries, which may not fully reflect global trends in combating digital crime. Secondly, the rapid evolution of technology and the constant emergence of new forms of cybercrime creates a risk that some conclusions and recommendations may need to be updated in the near future. Thirdly, the study is limited to the timeframe of 2023-2024, which may not fully reflect long-term trends in cybercrime. It is also worth noting the limitations associated with access to confidential information on the methods of operational and investigative activities, which could affect the completeness of the analysis of some aspects of the research.

REFERENCES

Adyrna.kz. (2024). *A new department has been established within the Ministry of Internal Affairs*. https://adyrna.kz/en/post/1007806

AIDARBAYEV, S., & UDERBAYEVA, B. (2020a). The Chinese 'Belt and Road' and Kazakhstan's 'Nurly Zhol': Legal and political aspects of cooperation within two initiatives. In: *The challenge of change for the legal and political systems of Eurasia: Eurasiathe impact of the new silk road* (pp. 119-132). Peter Lang AG

AIDARBAYEV, S., & UDERBAYEVA, B. (2020b). The Chinese 'Belt and Road' and Kazakhstan's 'Nurly Zhol': Legal and political aspects of cooperation within two initiatives. In: *The challenge of change for the legal and political systems of Eurasia: The impact of the new silk road* (pp. 117-129). Peter Lang AG

AKHMETOV, D.T., & RYSMAGAMBETOVA, G.M. (2022). Legal aspects of law enforcement operative-investigative activity in special conditions in

Kazakhstan. *International Journal of Electronic Security and Digital Forensics*, *14*(2), 199-208. https://doi.org/10.1504/IJESDF.2022.121179

ALIKHANOV, A., & BUSURMANKULOVA, U. (2022). Threats and challenges to the economic security of the state in the context of digitalization. *Bulletin of the Jusup Balasagyn Kyrgyz National University,* *14*(2), 389-394. https://balasagynbulletin.com/en/journals/tom-14-2-2022/ugrozy-i-vyzovy-ekonomichyeskoy-byezopasnosti-gosudarstva-v-usloviyakh-tsifrovizatsii

ALIMKULOV, Y., SHARIPOVA, A., ZHANIBEKOV, A., MUKHAMADIYEVA, G., & ARYN, A. (2023). Private detective activity of the law enforcement system of Kazakhstan on the experience of foreign countries. *International Journal of Electronic Security and Digital Forensics*, *15*(6), 644-654. https://doi.org/10.1504/IJESDF.2023.133964

APAKHAYEV, N., OMAROVA, A.B., KUSSAINOV, S., NURAHMETOVA, G.G., BURIBAYEV, Y.A., KHAMZINA, Z.A., KUANDYKOV, B., TLEPINA, S.V., & KALA, N.S. (2018). Review on the outer space legislation: Problems and prospects. *Statute Law Review, 39*(3), 258-265. https://doi.org/10.1093/slr/hmx010

BITAAB, M., CHO, H., OEST, A., ZHANG, P., SUN, Z., POURMOHAMAD, R., KIM, D., BAO, T., WANG, R., SHOSHITAISHVILI, Y., DOUPÉ, A., & AHN, G. (2021). Scam pandemic: How attackers exploit public fear through phishing. https://arxiv.org/abs/2103.12843

BOLATBEK, M., BAISPAY, G., MUSSIRALIYEVA, S., & USMANOVA, A. (2024). A framework for detection and mitigation of cyber criminal activities using university networks in Kazakhstan. *Radioelectronic and Computer Systems*, *2*(110), 186-202. https://doi.org/10.32620/reks.2024.2.15

Budapest Convention on Cybercrime. (2001). https://rm.coe.int/1680081561

CHERTOFF, M., & REDDY, D.S. (2022). Digital technology and police investigations: Challenges and opportunities in cross-border cybercrime. *Security Journal*, *35*(2), 320-338. https://doi.org/10.1057/s41284-021-00289-z

CHOO, KK.R. (2008). Organised crime groups in cyberspace: A typology. *Trends in Organized Crime*, *11*(3), 270-295. https://doi.org/10.1007/s12117-008-9038-9

Committee on Legal Statistics and Special Accounts of the Prosecutor General's Office of the Republic of Kazakhstan. (2023). *Criminal offenses:*

Statistics on the most important indicators of registered criminal offenses. https://qamqor.gov.kz/crimestat/indicators

Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism. (2005). https://rm.coe.int/168008371f

Criminal Procedure Code of the Republic of Kazakhstan. (2014). https://adilet.zan.kz/eng/docs/K1400000231

Cybersecurity Act. (2018). https://sso.agc.gov.sg/Act/CA2018

Cybersecurity Act. (2023). https://www.riigiteataja.ee/en/eli/519082024019

DI NICOLA, A. (2022). Towards digital organized crime and digital sociology of organized crime. *Trends in Organized Crime*. https://doi.org/10.1007/s12117-022-09457-y

DZIUBYNSKYI, A., POBEREZHNA, Z., SHEHYNSKYI, O., PAKHOLIUK, O., & RIZNYK, D. (2024). Management of Transport and Logistics Systems: Problems Under Conditions of Military Operations. *Lecture Notes in Networks and Systems, 1080*, 363-373. https://doi.org/10.1007/978-3-031-67444-0_35

European Union Agency for Cybersecurity (ENISA). (2023). *ENISA threat landscape 2023*. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

GARCIA, E., & BROWN, T. (2022). Artificial intelligence applications in digital crime investigation: A systematic review. *Journal of Police and Criminal Psychology*, *36*(3), 616-626. https://doi.org/10.1007/s11896-021-09468-5

HOLT, T.J., CALE, J., LECLERC, B., & DREW, J. (2020). Assessing the challenges affecting the investigative methods to combat online child exploitation material offenses. *Aggression and Violent Behavior*, *55*, 10146. https://doi.org/10.1016/j.avb.2020.101464

HORAN, C., & SAIEDIAN, H. (2021). Cyber crime investigation: Landscape, challenges, and future research directions. *Journal of Cybersecurity and Privacy*, *1*(4), 580-596. https://doi.org/10.3390/jcp1040029

KAIYRBEKOVA, G. (2024). Criminal legal measures to counteract the activities of financial pyramids in the Republic of Kazakhstan. *Pakistan Journal of Criminology*, *16*(3), 153-170. https://doi.org/10.62271/pjc.16.3.153.170

KASSYMZHANOVA, A.A., USSEINOVA, G.R., BAIMAKHANOVA, D.M., IBRAYEVA, A.S., & IBRAYEV, N.S. (2022). Legal framework for external security of the Republic of Kazakhstan. *International Journal of Electronic Security and Digital Forensics*, *14*(2), 209-222. https://doi.org/10.1504/IJESDF.2022.121180

KEMP, S., BUIL-GIL, D., MONEVA, A., MIRÓ-LLINARES, F., & DÍAZ-CASTAÑO, N. (2021). Empty streets, busy internet: A time-series analysis of cybercrime and fraud trends during COVID-19. *Journal of Contemporary Criminal Justice*, *37*(4), 480-501. https://doi.org/10.1177/10439862211027986

KHAMZIN, A., KHAMZINA, Z., MUKHAMEDZHANOV, O., TAITORINA, B., & BURIBAYEV, Y. (2023). Human Trafficking: Problems of Counteraction in Kazakhstan. *Access to Justice in Eastern Europe*, *4*(21). https://doi.org/10.33327/AJEE-18-6.4-a000404

KOSHKINBAEVA, A.S., SHAIGALIYEV, M.G., BURIBAYEV, Y.A., KHAMZINA, Z.A., & KHAMZINA, S.S. (2019). International legal regulation of environmental safety: In focus – Kazakhstan. *Rivista di Studi Sulla Sostenibilita, 1*, 121-142. https://doi.org/10.3280/RISS2019-001008

LALLIE, H.S., SHEPHERD, L.A., NURSE, J.R., EROLA, A., EPIPHANIOU, G., MAPLE, C., & BELLEKENS, X. (2020). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & Security*, *105*, 102248. https://doi.org/10.1016/j.cose.2021.102248

Law of the Republic of Kazakhstan No. 418-V "On Informatisation". (2015). https://adilet.zan.kz/eng/docs/Z1500000418

Law of the Republic of Kazakhstan No. 54-XIII "On Operational and Investigative Activities". (1994). https://adilet.zan.kz/kaz/docs/Z940004000_

Law of the Republic of Uzbekistan No. LRU-344 "On Operational Investigative Activities". (2012). https://lex.uz/docs/-2107763

LEUKFELDT, E.R., & HOLT, T.J. (2020). Examining the social organization practices of cybercriminals in the Netherlands online and offline. *International Journal of Offender Therapy and Comparative Criminology*, *64*(5), 522-544. https://doi.org/10.1177/0306624X19895886

MEHLA, A., & MEHLA, L. (2024). The Telecommunications Act, 2023: Solidarity Between Democracy and Totalitarianism. *Statute Law Review, 45*(2), hmae032. https://doi.org/10.1093/slr/hmae032

MITSKAYA, E.V., & SHKABIN, G.S. (2021). Criminal legal regulation of lawful infliction of harm in the course of covert actions of law enforcement agencies: Legislative experience of the Republic of Kazakhstan. In: G. SHKABIN, U. HELMANN, & V. LEZER (Eds.), *Proceedings of the VII International Scientific-Practical Conference "Criminal Law and Operative Search Activities: Problems of*

Legislation, Science and Practice" (pp. 214-218). Moscow: Research Institute of the Federal Penitentiary Service of Russia. https://doi.org/10.5220/0010634000003152

National Cyber Security Index (NCSI). (2025). *Kazakhstan*. https://ncsi.ega.ee/country/kz/

Normative Resolution of the Supreme Court of the Republic of Kazakhstan No. 8 "On Amendments and Supplements to Certain Regulatory Resolutions of the Supreme Court of the Republic of Kazakhstan on Criminal and Criminal Procedure Legislation". (2018). https://adilet.zan.kz/kaz/docs/P180000008S

Normative Resolution of the Supreme Court of the Republic of Kazakhstan No. 1 "On Certain Issues of Sanctioning Preventive Measures". (2020). https://adilet.zan.kz/kaz/docs/P200000001S

OMELCHUK, O.M., HAIUR, I.Y., KOZYTSKA, O.G., PRYSIAZHNA, A.V., & KHMELEVSKA, N.V. (2022). Analysis of the activities of law enforcement authorities in the field of combating crime and corruption offences. *Journal of Money Laundering Control*, *25*(3), 700-716. https://doi.org/10.1108/JMLC-07-2021-0073

Organisation for Economic Co-operation and Development (OECD) Guidelines on Digital Security Risk Management. (2025). https://www.oecd.org/en/topics/digital-security-risk-management.html

Organisation for Security and Co-operation in Europe (OSCE). (2024). *First meeting of the Interagency Steering Committee to Counter Cybercrimes in Kazakhstan*. https://www.osce.org/programme-office-in-astana/566881

Resolution of the Government of the Republic of Kazakhstan No. 407 "On Approval of the Cybersecurity Concept "Cybershield of Kazakhstan". (2017). https://adilet.zan.kz/kaz/docs/P1700000407

SANIYAZOVA, Y., MEDIYEV, R., SAITOVA, E., UTEGENOVA, G., & KZYLKHOJAYEVA, A. (2024). Advancing forensic science in Kazakhstan: The emergence and impact of digital forensics in cybercrime investigation. *Law, State & Telecommunications Review*, *16*(2), 48-68. https://doi.org/10.26512/lstr.v16i2.49190

SARKAR, G., & SHUKLA, S.K. (2023). Behavioral analysis of cybercrime: Paving the way for effective policing strategies. *Journal of Economic Criminology*, *2*, 100034 https://doi.org/10.1016/j.jeconc.2023.100034

SEITZHANULY, G., BACHURIN, S.N., AITUAROVA, A.B., GASSANOV, A.A., & SYRBU, A.V. (2022). Confidentiality in the activities of law enforcement agencies and the court during covert investigative activities.

International Journal of Electronic Security and Digital Forensics, *14*(2), 151-164. https://doi.org/10.1504/IJESDF.2022.121192

SEMENENKO, O., MARKO, I., CHERNYSHOVA, I., KOVERGA, V., & PEKULIAK, R. (2021a). Methodological Aspects of the Military-Economic Significance of Agriculture and Modern Problems of Military Food Resources in Ukraine. *Scientific Horizons, 24*(8), 81-97. https://doi.org/10.48077/scihor.24(8).2021.81-97

SEMENENKO, O., MINOCHKIN, A., VASYLENKO, S., KLEPIKOV, V., & PRAVDYVETS, O. (2021b). Assessment of the Impact of the Armed Conflict in Ukraine on the Development of the Agricultural Sector and Price Setting. *Scientific Horizons, 24*(7), 68-80. https://10.48077/scihor.24(7).2021.68-80

SHAISULTANOV, S., AKIMZHANOV, T., ABDRAKHMANOV, B., BAZARLINOVA, A., & BAZARLINOVA, A. (2024). Combating internet fraud through operative-search measures. *Law, State & Telecommunications Review*, *16*(2), 257-275. https://doi.org/10.26512/lstr.v16i2.50740

SHAKEEVA, N., ANDASHOVA, R., & JUMALIEVA, G. (2025). Intercultural communication in digital space: Challenges and adaptation strategies. *Bulletin of the Jusup Balasagyn Kyrgyz National University, 17*(3), 59-67. https://doi.org/10.58649/1694-8033-2025-3(123)-59-67

SMAILOV, N., KADYROVA, R., ABDULINA, K., URALOVA, F., KUBANOVA, N., & SABIBOLDA, A. (2025a). Application of facial recognition technologies for enhancing control in information security systems. *Informatyka, Automatyka, Pomiary w Gospodarce i Ochronie Srodowiska, 15*(3), 55-58. https://doi.org/10.35784/iapgos.7073

SMAILOV, N., TOLEMANOVA, A., AZISKHAN, A., SEKENOV, B., & SABIBOLDA, A. (2025b). Implementation of fiber-optic sensing systems in structural health monitoring of concrete. *Informatyka, Automatyka, Pomiary w Gospodarce i Ochronie Srodowiska, 15*(3), 73-76. https://doi.org/10.35784/iapgos.7606

SULTANBAYEVA, G.S., Turdubaeva, E.O., Lozhnikova, O.P., & Tastemirova, G.A. (2023). Developing a platform for cross-border investigative journalism in Central Asia. *Herald of Journalism*, *68*(2), 72-81. https://doi.org/10.26577/HJ.2023.v68.i2.07

United Nations (UN) Convention against Transnational Organised Crime. (2004). https://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-e.pdf

VAN DER WAGEN, W., & PIETERS, W. (2020). The hybrid victim: Re-conceptualizing high-tech cyber victimization through actor-network

theory. *European Journal of Criminology*, *17*(4), 480-497. https://doi.org/10.1177/1477370818812016

ZHAKENOV, K., KULTEMIROVA, L., & IBRAEVA, A. (2024). Comparative analysis of the activities of authorities to ensure the prevention of offenses in the Republic of Kazakhstan and other world countries. *Security Journal*, *37*(4), 1430-1446. https://doi.org/10.1057/s41284-024-00425-5

ZHAKUPOV, Y. (2024). Criminological aspects of business protection in the Republic of Kazakhstan. *Pakistan Journal of Criminology*, *16*(3), 495-512. https://doi.org/10.62271/pjc.16.3.495.512

ZHAMIYEVA, R.M., & ALBEKOVA, M.G. (2023). AML in Kazakhstan: Progress, challenges and future prospects. *Bulletin of the Karaganda University "Law Series"*, *110*(2), 75-81. https://doi.org/10.31489/2023L2/75-81

ZHAMIYEVA, R.M., SULTANBEKOVA, G.B., ABZALBEKOVA, M.T., ZHAKUPOV, B.A., & KOZHANOV, M.G. (2022). The role of financial investigations in combating money laundering. *International Journal of Electronic Security and Digital Forensics*, *14*(2), 188-198. https://doi.org/10.1504/IJESDF.2022.121183

The Law, State and Telecommunications Review / Revista de Direito, Estado e Telecomunicações

Contact:
Universidade de Brasília - Faculdade de Direito - Núcleo de Direito Setorial e Regulatório
Campus Universitário de Brasília
Brasília, DF, CEP 70919-970
Caixa Postal 04413

Phone: +55(61)3107-2683/2688

E-mail: getel@unb.br

Submissions are welcome at: https://periodicos.unb.br/index.php/RDET