MULTIDISCIPLINARY SCIENTIFIC RESEARCH
BJMSR VOL 11 NO 1 (2026) P-ISSN 2687-850X E-ISSN 2687-8518
Available online at https://www.cribfb.com
Journal homepage: https://www.cribfb.com/journal/index.php/BJMSR
Published by CRIBFB, USA

LEGAL REGULATION OF CYBERATTACKS AND CYBERCRIME: ANALYSIS OF JUDICIAL PRACTICE AND COUNTERACTION STRATEGIES

Volodymyr Warawa [(a)] *Vladyslav Honcharuk* [(b)1] *Oleksandra Kozlovska* [(c)] *Dina Dryzhakova* [(d)] *Valentyn Vyshnevskyi* [(e)]

[(a)]*Associate Professor, Chamber of Operative and Searching Activity, Faculty of Preparing Specialists for Divisions of Criminal Police, National Police of Ukraine, Dnipro State University of Internal Affairs, Dnipro, Ukraine; E-mail: warawa@ukr.net*
[(b)]*Associate Professor, Chamber of Information and Financial Security, Institute of Security PJSC "Interregional Academy of Personnel Management" (IAPM) Kyiv, Ukraine; E-mail: xrixos@gmail.com*
[(c)]*Lecturer, Department of Intellectual Power and Private Law, National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine; E-mail: dasha7770@ukr.net*
[(d)]*Graduate Student, Department of Criminal Legal Policy and Criminal Law, Taras Shevchenko National University of Kyiv, Kyiv, Ukraine; E-mail: d.dryzhakova@gmail.com*
[(e)]*Candidate of Science of Law, Head of the Maritime Law Department, Educational and Scientific Institute of Maritime Law and Management, National University "Odessa Maritime Academy", Odesa, Ukraine; E-mail: bespeka.ua@gmail.com*

ARTICLE INFO

Article History:

Received: 20th June 2025
Reviewed & Revised: 20th June 2025 to 28th September 2025
Accepted: 30th September 2025
Published: 4th October 2025

Keywords:

Court Practice, Cybercrime, Digital Money, Digital Security, Fraud, Innovative Technologies

JEL Classification Codes:

K24, L86

Peer-Review Model:

External peer review was done through double-blind method.

ABSTRACT

Rapid digitalization processes in public life have led to a sharp increase in the scale of cybercrime, posing a threat to economic stability, data privacy, and national security. The problem is becoming particularly relevant in Ukraine in the context of hybrid threats associated with Russian aggression and the intensification of cyberattacks. The purpose of this study was to analyze the legal regulation of cyberattacks and cybercrimes based on Ukraine's judicial practice, identifying characteristic features and trends in the development of law enforcement. To achieve the goal, a systematic review of scientific sources, national and international regulatory acts, and an analysis of selected court decisions were used. The selection of materials was carried out using the PRISMA methodology. The methods of content analysis, comparison, and synthesis were used to process the sources. Scientific publications and court cases related to cybercrimes from 2019 to 2023, as well as international conventions, were considered. The results show that after the Russian invasion, the number of registered cybercrime cases increased. Phishing has become especially popular, accounting for over half of all cases. Most of the crimes were of a cross-border nature. As judicial practice has shown, cybercrime in Ukraine has characteristic features: it is international, and almost all cases involve financial fraud. The main findings indicate that the judicial practice of Ukraine demonstrates the predominance of fraudulent cybercrimes, a significant share of which is phishing, as well as systemic difficulties with the procedural provision of electronic evidence.

INTRODUCTION

The active development of innovative information technologies has resulted from the general, global digitalization of social life. At the same time, improvements in document management, finance, and the robotization of production and services are closely linked to cybersecurity, which is becoming increasingly crucial in the context of total digitalization. Cyberattacks and cybercrime have become serious challenges for government agencies, private companies, and individuals (Erikha & Saptomo, 2024). The use of cyberattacks has become a powerful weapon that can cause significant damage not only to economic life but also to national security agencies, information privacy rules, and public life in general. In today's environment, countering such phenomena has become one of the key challenges for the functioning of national legal systems in any state and the operation of international law in the globalized context. Hence, the use of cyberattacks is increasingly becoming a tool that can cause paralysis of critical infrastructure, result in significant economic losses, and pose a threat to

[1]*Corresponding Author: ORCID ID: 0000-0002-9627-9530*

https://doi.org/10.46281/bjmsr.v11i1.2651

To cite this article: Warawa, V., Honcharuk, V., Kozlovska, O., Dryzhakova, D., & Vyshnevskyi, V. (2025). LEGAL REGULATION OF CYBERATTACKS AND CYBERCRIME: ANALYSIS OF JUDICIAL PRACTICE AND COUNTERACTION STRATEGIES. *Bangladesh Journal of Multidisciplinary Scientific Research*, *11*(1), 1-12. https://doi.org/10.46281/bjmsr.v11i1.2651

national security.

Legal regulation in cybersecurity encompasses a wide range of measures, from introducing specific legal provisions on liability for cyberattacks and cybercrime to developing relevant strategies to prevent such actions and mitigate their devastating consequences (Kethineni, 2020; Artemchuk et al., 2024). In general practice, both criminal law aspects and administrative or civil law approaches are used. First, the key challenges in ensuring effective investigations of existing cybercrimes and establishing jurisdiction in international violations are harmonizing national legal systems and legislation with international standards. In this context, an essential element is to consider the existing analysis of judicial practices, which will allow us to assess the effectiveness of current regulations, identify specific gaps in the legal system, and propose possible solutions to improve the current situation (Hummelholm, 2022). In Ukraine, studying case law also provides opportunities to track the evolution of approaches to qualifying cyberattacks, identify areas for understanding responsibility, and implement specific preventive measures (Batrachenko et al., 2024). However, the key problems remain the harmonization of national legislation with international standards and determining jurisdiction in cases with a cross-border element. At the same time, in the context of the war against Ukraine, this problem has become particularly relevant, since the number of registered cybercrimes has increased significantly, and judicial practice reveals special difficulties in their qualification and proof. This approach is essential for analyzing successful practices of preventing digital crimes in the context of Russian aggression (including hybrid challenges of digital attacks). This includes the application of legal expertise from various countries, the coordination of interactions with international law enforcement institutions (Khalymon et al., 2019), and the implementation of specific standards developed as part of the Budapest Convention on Cybercrime, among other initiatives.

The scientific problem arises in clarifying the effectiveness of legal mechanisms for countering cyberattacks and cybercrimes at the national and international levels. The purpose of the study is to analyze the judicial practice of Ukraine in the field of cybercrime and the application of a characteristic feature of law enforcement. The realization of this goal involves the following tasks: 1. Determination of the general state of countering cybercrime in Ukraine, study of current regulations in this area (national and international). 2. Analysing the most common types of fraud and existing judicial practice on the punishment of criminals. The work uses the PRISMA methodology for selecting sources and methods of content analysis, comparison, and synthesis to generalize the results. The central research hypothesis is that a comprehensive approach that combines legislative, technical, and organizational measures has the potential to ensure an adequate level of cyber protection in the modern world.

The article is structured as follows: the first section provides an overview of modern scientific and legal approaches to cybercrime; the second section presents the results of an analysis of Ukrainian judicial practice; the third section discusses the findings; and the final section presents the conclusions.

LITERATURE REVIEW

The legal regulation of cybercrime is formed at the intersection of national and international legal systems and is a subject of active scientific discussion. At the same time, a significant portion of modern research emphasizes the need to combine international and national instruments to ensure effective countermeasures against digital threats. Pettoello-Mantovani (2024) pointed out that such issues require in-depth judicial review, suggesting the possibility of using the International Criminal Court for violations in digital space. However, not all researchers support the thesis that international justice is essential. For example, Spassova (2023) believes that it is sufficient to use the national competence of courts to bring criminals to justice. In contrast to global justice systems, she emphasizes the importance of deep cooperation between courts and law enforcement agencies of different countries, which will be the basis for further investigative and judicial actions. This view is supported by Wessel and Heim (2023), who emphasize the problematic aspects of using an international judicial organization due to the challenges of establishing a unified legal framework for such an institution's work. Alexandrou (2021) carried out a separate systematic analysis of international laws and standards. National legal systems are more flexible and have extensive networks of courts that effectively regulate legal issues throughout the country. Dragojlović (2023) also actualized the problem of extending judicial jurisdiction in cases related to digital offenses. He proposed a compromise option, considering the norms of national legal systems while utilizing international standards to regulate the issue of cybercrime in the international arena. Against the backdrop of such discussions, Ukrainian cases are somewhat overshadowed, which can also be attributed to the issue of the effectiveness of the legal framework in Ukraine for punishing cybercriminals.

Separately, the researchers aimed to summarize existing experiences regarding the possibility of forming certain generalizations. We refer to the study by Kagita et al. (2021), which conducted an in-depth analysis of cybercrime in the Internet of Things, characterized the specific legal concepts used in such a system, and highlighted existing legal protection mechanisms based on examples from Asian court decisions. Similarly, Asian legal practice was analysed by Li and Liu (2021), who conducted a thorough review of the scientific literature on combating digital crimes at the national and international levels (with an emphasis on Chinese legal proceedings). Noor Uddin Milon et al. (2024) highlighted the methodological capabilities of the PRISMA scientific method for classifying cybercrime, identified some challenges in applying this approach, and outlined prospects for further scientific investigation. The final study by Verma and Shri (2022) provides an overview of the possibilities of controlling and counteracting digital offenses. They identified some of the challenges law enforcement faces in protecting against cyberattacks. The researchers also characterized the active growth of cyber challenges in the post-COVID-19 pandemic era, which is attributed to the introduction of remote services, digital documentation, and other factors. At the same time, Mezei and Szentgály-Tóth (2023) highlighted the threat of cyberattacks on online platforms, as this area is largely unregulated by law, primarily due to the rapid development of online platforms

outpacing legislative regulation. In a legal vacuum, court decisions can serve as specific markers to guide future legislative initiatives. Some crucial conclusions are contained in the summarizing papers on the legal experience of countering cyber threats in individual countries. The original systems of South Africa and Indonesia, whose governments closely monitor the current digital challenges, offer separate legal solutions to define individual and collective criminal acts (Snail Ka Mtuze & Musoni, 2023). Although the studies presented here are generalizable, their results are critical for considering international experience in regulating digital crimes. Instead, these studies focus on the Asian experience of countering such cases, whereas the Ukrainian context requires improved assessments.

The study by Baranovska (2024), which examines the current challenges to Ukraine's cybersecurity and highlights the potential solutions to counter the latest threats (including the hybrid threat posed by the aggressive Kremlin regime), is crucial for understanding the Ukrainian law enforcement system. Instead, other studies have identified the crisis of modern culture through the lens of philosophical vision, which is also related to relationships in the digital space (Borysenko et al., 2024). The researchers determined that, in some cases, the inability to behave appropriately in the digital world can lead to falling prey to criminals. At the same time, authors emphasized the need to develop digital security through the lens of the widespread adoption of digital currency in Ukraine and its increasing use in payment transactions (Tumalavičius, 2022). The results obtained by the researchers can be compared with the European experience, as summarized in Danidou's (2020) work, which identified the importance of a harmonized legal framework as a key factor in building a strong financial market in the international space. Similar conclusions were drawn by other authors, who highlighted the importance of legal protection for agricultural operations and related economic sectors (Lavrov et al., 2022). In a globalized digital society, such problems are becoming global and beyond the Ukrainian legal framework. However, this issue will require further study, as the discussion points proposed by the authors have not yet been adequately evaluated in the scientific literature. In Ukrainian realities, however, the importance of using digital attacks as a side effect of Russian military aggression has been emphasized (Kozlovskyi et al., 2023). Similarly, scholars emphasize certain court decisions that have theoretical value in countering cyberattacks in the short term (Cherniavskyi et al., 2021). This issue remains relevant, as digital offenses are evolving in tandem with innovative technologies, necessitating the continuous development of theoretical knowledge to combat existing challenges.

Moreover, modern research has shown that the problem of legal regulation of cybercrime goes far beyond criminal law and concerns the functioning of the judicial system as a whole. One of the key topics is the issue of conflict of interest in the activities of judges, which directly affects the quality of consideration of cases related to digital offenses. A comparative analysis of Ukrainian and European practice has shown that the lack of precise mechanisms for preventing conflicts reduces trust in judicial decisions in the field of digital security and requires greater transparency in law enforcement (Shevchuk et al., 2023a; Shevchuk et al., 2023b). A separate layer of research focuses on hybrid wars, in which cyberattacks have become an important tool. An analysis of international experience has shown that the combination of military and cyber operations creates legal dilemmas for states and international organizations, particularly regarding the jurisdiction and qualification of the actions of attackers (Simons, Danyk, & Maliarchuk, 2020). Research in African countries has shown that developing specialized laws in the field of cybersecurity can be effective even with limited resources. The legal system of South Africa has demonstrated an example of an active legislative response to the growth of cybercrime, laying the groundwork for a comprehensive counteraction to digital threats (Snail ka Mtuze & Musoni, 2023). The legal regulation of attacks on satellite communications has also become an important aspect. Researchers have emphasized the blurring of the boundaries between cybercrime and interference with technology. This fact presents new challenges for lawyers to develop a unified approach to qualifying such actions (Spassova, 2023). The institutional approach to countering digital threats is also evident within administrative law. Ukraine's experience has demonstrated the need to establish separate mechanisms that effectively combat corruption in the field of territorial defense, which also has a cyber dimension in terms of ensuring digital infrastructure (Sysoiev et al., 2024). Research on digital currencies deserves special attention. The challenges associated with blockchain projects and cryptocurrencies underscore the lack of a unified international legal framework, which complicates the protection of user rights and creates conditions for digital crimes in the realm of financial relations (Tumalavičius, 2022). Generalizing studies at the international level have indicated a wide range of digital threats. In particular, reviews of modern crimes in the field of cybersecurity have indicated uneven legal responses, the lack of unified protection measures, and the constant evolution of attack methods (Verma & Shri, 2022).

The theoretical basis for studying cybercrime is also provided by a fundamental monograph, which reveals the peculiarities of the interaction between cybercrime and cybersecurity on a global scale. The author emphasizes that the dynamism of digital threats significantly exceeds the pace of legal regulation (Watters, 2023).

A separate area of research concerns the inconsistency in international regulation of cyber threats. The lack of consistency between different legal systems leads to the problem of fragmented approaches, which in turn complicates effective investigation and the pursuit of justice for perpetrators (Wessel & Heim, 2023).

Summarizing the above sources, modern research highlights various international and national aspects of the legal regulation of cybercrime. They have employed a variety of approaches, ranging from global institutional decisions to local judicial practices. At the same time, a common feature is the recognition of the law's lack of adaptability to the rapid development of digital technologies, which forms the basis for further research. Moreover, the lack of consensus on cybercrime law enforcement and regulation creates a basis for further research. Additionally, there is a lack of analysis of judicial practice in cybercrime, despite some studies on cybercrime case law. Therefore, this study aims to help close these gaps, analyze judicial practice through the lens of law enforcement effectiveness in cybersecurity, and formulate recommendations for enhancing mechanisms for bringing cybercriminals to justice.

MATERIALS AND METHODS

Research Design

The type of research is mixed, combining a systematic review of scientific sources with a review of legal cases. The case study approach was chosen as it is the most suitable method for examining the realities of judicial practice in a specific country. Additionally, this approach was chosen because it enables us to examine specific cases of cybercrime litigation, thereby helping to determine the effectiveness of current legislation, court decisions, and law enforcement practices (Ahmad et al., 2024). This is especially important in the constant evolution of digital threats. The analysis incorporates court case materials, legislative acts, and scholarly literature. This study aims to provide new insights into the most common judicial cases related to cybercrime and characterize the typical features of cybercriminal activities.

Materials

Various sources were selected for inclusion, including accessible court cases, legislative acts, and scholarly literature. The sampling of materials was purposive and based on pre-established inclusion criteria. These criteria addressed aspects such as the type of case, time frame, availability of materials, relevance, validity, alignment with the research topic, and language of publication. Specific considerations included jurisdiction, type of case, duration of proceedings, and the availability of court cases for inclusion. Different criteria were developed for including legislative acts, focusing on their relevance, validity, and the hierarchical level of the normative legal act. These criteria were formulated to ensure the inclusion of the most relevant and up-to-date laws for studying the specific features of cybercrime regulation. Table 1 provides an overview of the key inclusion criteria for the materials.

Table 1. Criteria for inclusion of court cases

No.	Criterion	Description	The type of materials
1	Jurisdiction	Court cases that were considered in the courts of Ukraine	Court cases
2	Case type	Court cases related to cybercrime or international legal assistance in the field of cybercrime	Court cases
3	The term of consideration	Cases reviewed for 2023-2024. Scientific literature from 2019 to 2024	Court cases
4	Accessibility	Publicly available court decisions or materials that allow for a thorough analysis were included. Publicly available scientific literature	Court cases Nonfiction
5	Accessibility	Works or legislative acts describing the specifics of the regulation of the issue of cybersecurity or the protection of personal data	Nonfiction Legislative acts
6	Accessibility	Documents that are valid at the time of the research	Legislative acts
7	Regulatory and legal level	National laws and government regulations are included	Legislative acts
8	Subject	Materials devoted to issues of cyber security, cyberspace protection, legal regulation, or the study of judicial practice The materials highlight the peculiarities of judicial practice implementation in Ukraine.	Court cases, Legislative acts Nonfiction
9	Source type	Monographs, scientific articles in peer-reviewed journals, reviews, and conferences General theoretical works, in which it is difficult to identify the type, were not eligible for inclusion.	Nonfiction
10	Language of writing	Ukrainian, English For scientific literature, the presence of an English-language annotation is mandatory.	Court cases Nonfiction
11	Authority	Studies written by leading researchers Works published in peer-reviewed journals	Nonfiction

Source: Authors' Elaboration

Thus, using these criteria, court cases, legislative acts, and scholarly literature were selected for analysis, with a focus on issues related to cybersecurity, cyberspace protection, legal regulation, and judicial practice studies.

Procedure and Tools

The PRISMA approach was employed for processing and screening scientific materials (Figure 1). This approach is widely used in academic research to select and analyse the most relevant scholarly literature and other sources. Initially, Scopus and Google Scholar were chosen as the scientometric databases. Search queries included keywords such as cybersecurity, digital data protection, judicial practice, courts, penalties, Ukraine, EU, and challenges. A total of 3,367 results were obtained.

First, all duplicates were removed (-1,156), leaving 2,211 items of scholarly literature for screening. The next step involved screening all sources based on their abstracts and keywords, excluding 789 items. An additional 510 items were excluded because they were deemed irrelevant to the research topic. Subsequently, the main inclusion criteria were applied. Several legislative acts, relevant websites, and platforms containing court cases (30 items) were identified through the search engines. Court cases were located on the Opendatabot platform using the keyword "cybersecurity." After screening, nine court cases and several laws were selected from the platform.

The principal collected cases focused on the following areas. Cases related to cyberattacks or cybercrimes. 2. Cases demonstrating typical challenges in law enforcement. 3. Decisions that established significant precedents in the field of cybercrime. Additionally, information from one website providing general statistical data was included.

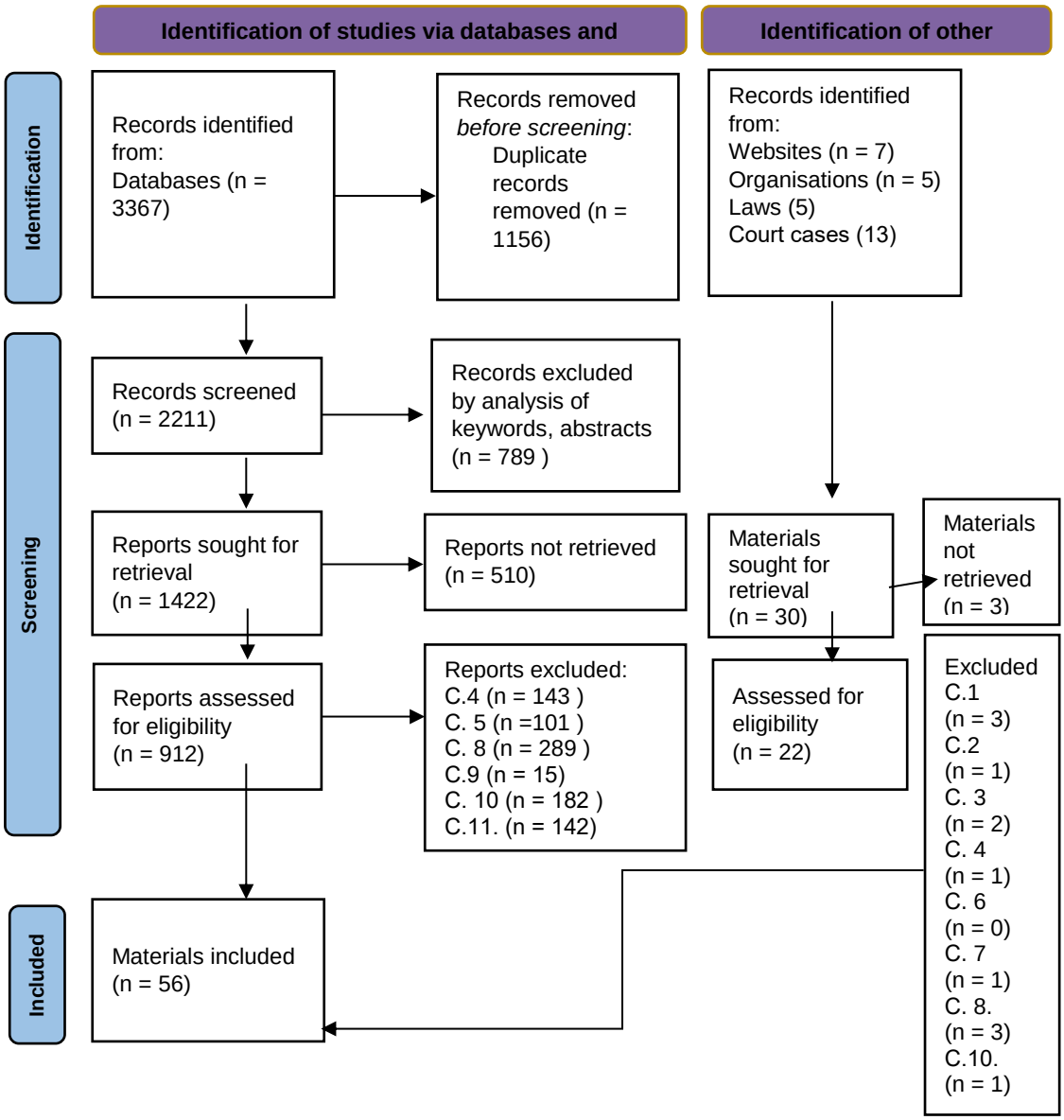

Figure 1. The step-by-step screening and selection of materials

Data Analysis

A systematic organization and classification by specific thematic categories was conducted using the PRISMA methodological approach to analyze the collected materials. Qualitative analysis was performed using Google Sheets software. Specifically, three spreadsheets were created within the program.

The first spreadsheet focused on scholarly literature and included the following components: author, year of publication, cybersecurity features, definitions of cybercrime, and descriptions of judicial practice. The second spreadsheet addressed key legislative acts, consisting of the law number, adoption date, adaptation date, definitions of cybercrime, and other primary legislative regulations. The third spreadsheet pertained to court cases, including the case number, the name of the court where the case was heard, and the essence of the case, including its main aspects and conclusions.

Following the classification of the data, a qualitative analysis was conducted for each category. To present the findings clearly, graphs and tables were used to illustrate the distribution of cybercrimes by category, the distribution of court cases by topic, and the proportion of international versus national decisions in cybercrime cases. Additionally, a comparative method was employed to align court case data and legislative acts with insights from scholarly literature. This combination of visual representation and comparative analysis enabled a more precise comparison and synthesis of the collected data.

RESULTS

Analyzing current legislation, cybercrime is defined as an unlawful act committed through information and communication technologies, aimed at compromising the security of computer systems, networks, data, or information resources. Consequently, such crimes can cause harm to individuals, organisations, governments, or society (Mezzetti et al., 2024). Without specialised knowledge, detecting, recording, and seizing forensically relevant information about a cybercrime is difficult (Gajjar & Taherdoost, 2024). Cybercrime is characterised by an exceptionally high level of latency and rapid growth in the number of crimes (Watters, 2023). This is primarily due to the rapid spread of the Internet in various fields. The key

features of cybercrime are its transnational nature, technical complexity, speed of crime, and harm to large groups of people. The figure illustrates the primary characteristics of cybercrime (See Figure 2).

Transnational Activities	Use of innovative technologies	Speed of Crime	Large-scale harm
Criminals operate from anywhere in the world. This makes it difficult to detect and prosecute them.	Cybercrimes require specialized skills and the use of innovative technologies.	Crimes can be committed in a matter of seconds.	A single crime can affect thousands of people simultaneously

Figure 2. Main features of cybercrime

As of 2017-2018, more than half of the reported cyber frauds (42%) were related to the absence of payment or delivery (Buçaj & Idrizaj, 2024). This category primarily included purchases made from fraudulent online stores that the victim had never used before. Alternatively, it was concerned with promised payments that were never received. Approximately 28% of cybercrime involved the leakage of personal data and phishing. At the same time, identity theft, credit card fraud, and other cyberattacks were relatively rare (Despotović et al., 2023). Since 2022, phishing has become particularly popular, accounting for over half of online criminal activity. Since the emergence of email phishing, hackers have improved the system, so that researchers now distinguish several types of this cybercrime: smishing (using messages), phishing (using calls), and imitation of resources popular with users, such as websites of public organisations, charity websites, email sites, or payment services (see Table 2).

Table 2. Types of Cybercrimes

Type of cybercrime	**2017**	**2022**
Non-payment or lack of delivery	41.6%	9.2%
Personal data leakage	15.3%	10.4%
Non-payment or lack of delivery	41.6%	9.2%
Investment fraud	1.5%	5.4%
Technical support desk	5.4%	5.8%
Extortion	7.4%	7%
Card fraud	7.5%	4.1%
Personal information theft	8.7%	5%
Phishing	12.5%	53.2%

Source: Authors' Own Elaboration

Since the beginning of the full-scale invasion, the activity of cyber fraudsters in Ukraine has increased significantly (Kuzior et al., 2024). 11% of people have become victims of fraud since the start of the full-scale invasion. Women fell into the hacker trap more often than men. According to statistics, young people predominate among the victims of fraud, with 18-24 year olds (14%) and those aged 65 and above (11.5%) being the most affected. In 2022, the total amount of losses incurred by banks, merchants, and customers due to illegal actions involving payment cards increased by 47%. More than half of the losses were caused by social engineering. Thus, in Ukraine, since 2022, people have become victims of fraudsters because they have provided their card details, one-time passwords to confirm transactions, or basic data for logging into online banking. In general, most fraudulent incidents occur during transactions, such as the purchase or sale of goods online, accounting for more than 52%. Fraudulent phishing links were also popular, accounting for almost 19%. The list of common fraudulent manipulations includes hacking of social media accounts (12%) and telephone solicitation (10.2%) (see Figure 3).

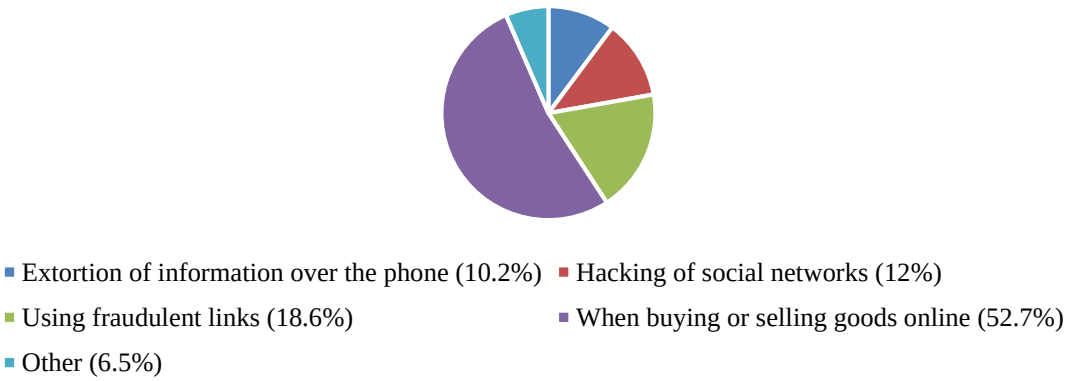

Figure 3. Types of cybercrimes in Ukraine
Source: Fintech Insider (2023)

Ten cases related to cybersecurity regulation were selected for analysis. The analysis of court practice in responding to cybercrime in Ukraine reveals that cases related to cybercrime exhibit several characteristic features. Cybercrime is a transnational phenomenon, as evidenced by the fact that criminals can often operate online from different parts of the world, and victims or affected individuals may be located in another country. Accordingly, this requires developing unique cooperation between states to respond effectively to such offences. In this case, based on the analysis of the court case documents, No. 1 of the Solomianskyi District Court of Kyiv or No. 2 of the Odesa Court of Appeal, Ukraine, provided international legal assistance to Slovenia in investigating a cybercrime that caused damage to a Slovenian citizen. In Ukraine, access to documents and things in such cases is granted based on Article 159 of the Criminal Procedure Code of Ukraine. This, in turn, requires temporary access to things and documents in the possession of a person or organisation that is part of an international criminal investigation (Kravtsov et al., 2024). The analysis of case No. 3 (Malynovskyi District Court of Odesa) outlines the detention of a person at the border on suspicion of committing a cybercrime. The legal basis for this was used: §1343 of Title 18 of the US Code (fraud, financial fraud), and the international wanted list was also confirmed by Interpol's blanks. Based on the analysis of Case No. 4 (Odesa Court of Appeal), a decision was made to extradite an Uzbek citizen to the United States for prosecution for cybercrime. Table 3 provides a detailed analysis of these cases.

Table 3. Analysis of court cases

No., Institution	The case	Main aspects	Other information
No. 1: Solomianskyi District Court of Kyiv	A citizen of Slovenia was a victim of cryptocurrency-related fraud. The cybercrime was committed through a platform that operated without the permission of the financial regulator, the FCA.	International component *Crime:* fraud: misrepresentation to gain access to cryptocurrencies Notification of the victim by a representative of the platform	Forming links between messages, the platform, and cryptocurrency transactions. Involvement of international cooperation mechanisms.
No. 2: Odesa Court of Appeal	Extradition of a citizen of Uzbekistan The US authorities want the person for fraud and cybercrime related to the theft of cryptocurrencies.	Risk of avoiding responsibility. The crimes correspond to Art. 190 of the Criminal Code of Ukraine (fraud) *Nature of the crime*: large-scale and international level.	The focus is on compliance with international standards for extradition. Ensuring the observance of human rights during the extradition process.
No. 3: Malynovskyi District Court of Odesa	Detention at the border on suspicion of committing a cybercrime	*Crime:* fraud: The legal basis is Section 1343 of Title 18 of the USA Code (fraud, financial fraud). *International search:* confirmation by Interpol records. Amount of loss: USD 11.8 million (theft of cryptocurrencies).	Prepare a professional extradition check in accordance with international standards and regulations. Ensure transparency of the process.
No. 4: Odesa Court of Appeal	The Prosecutor General of Ukraine has decided to extradite a citizen of Uzbekistan to the United States for prosecution on criminal charges related to cybercrime.	*Crime:* fraud: Main corpus delicti: financial fraud (analogous to Part 5 of Article 190 of the Criminal Code of Ukraine). Evidence: confirmation of the request by the US Department of Justice. Extradition: justified by a crime punishable by more than 1 year in prison.	It is essential to follow all procedures when transferring someone to the United States. The risks associated with appealing the extradition decision are also taken into account.
No. 5: Prymorskyi District Court of Odesa	Temporary arrest of a person wanted by the competent authorities of the United States of America for cybercrime	*Crime:* fraud The person is on the international wanted list The crimes the suspect is suspected of include fraud and cybercrime related to financial fraud.	Temporary arrest to ensure extradition.

Source: Unified Register of Court Decisions (2024)

On the other hand, an essential part of investigating cybercrime is collecting evidence from electronic systems (Ghimire, 2023). Cybercrime usually leaves electronic traces. Therefore, it is essential to consider data such as emails, correspondence, IP addresses, and transactions in electronic payment systems, among other relevant information. Accordingly, modern judicial authorities should have access to this information to collect evidence confirming the fact of the crime (Kelly & Montasari, 2023). In the case of Case No. 6, to collect evidence, the prosecutor applied to the court for temporary access to items and documents, including making copies of information from mobile terminals and computer systems used during the commission of the crime. Table 4 identifies the key aspects and additional information gathered from the analysis of other cases.

Table 4. Key aspects and additional information gathered from the analysis of other cases

No., Institution	Case	Key aspects	Other information
No. 6: Kherson City Court	An investigator's application for temporary access to bank documents related to a cybercrime resulted in the unlawful withdrawal of UAH 46,200 from the victim's account. The victim fell victim to a fraudulent scheme on the Telegram channel.	Corpus delicti: Part 3 Article 190 of the Criminal Code of Ukraine (fraud) Technical aspect of the fraud: phishing attack to gain access to bank data. Reasoning for the request: access to bank documents to verify transactions.	Paying attention to key technical evidence (phishing, changing the phone's 3DSecure) and ensuring that the investigation is supported by digital expertise.

No. 7: Commercial Court of Cassation of the Supreme Court	The plaintiff in the case is an agricultural enterprise that filed a lawsuit against the bank for unauthorized debiting of funds from its account. The case discusses cybersecurity and the bank's responsibility for protecting client funds.	Technical and financial capabilities. The bank has significantly greater cybersecurity capabilities than the claimant. The client has the right to protect their funds on the account, as provided for by the Constitution of Ukraine.	The Supreme Court recommends that the bank be obliged to ensure adequate security to prevent unauthorised financial transactions.
No. 8: Zmiivskyi District Court of Kharkiv Region	This case concerns criminal proceedings based on a crime under Article 185(4) of the Criminal Code of Ukraine (theft).	Extract from the Unified Register of Pre-trial Investigations confirming the fact of criminal proceedings. Report of the officer on duty about the cybercrime. A statement about the criminal offence. Protocol of interrogation of the victim. Images of a bank card that may be part of the evidence.	In this case, pursuant to Article 159 of the Criminal Procedure Code of Ukraine, temporary access to items and documents is granted for inspection, copying, or seizure.
No. 9: Shevchenkivskyi District Court of Kyiv	The case concerns unauthorised access to citizens' personal data by an employee of the bank's IT support department. The person accessed confidential information of the bank's clients and used it to commit financial crimes.	Temporary access to the bank's electronic systems was granted to verify log files and evidence of unauthorised transactions. The court agreed to the temporary access to the bank's data, as the electronic systems contained information about specific transactions and abuses.	The court granted the prosecutor's request and allowed temporary access to the bank's relevant electronic systems to facilitate the collection of evidence. Court practice shows the importance of controlling the collection of electronic evidence in cybercrime. This enables the effective investigation of such cases without compromising the rights of citizens.

Source: Unified Register of Court Decisions (2024)

Therefore, in counteracting, documenting, and investigating certain cybercrime-related offences, using electronic images as evidence in criminal proceedings is becoming a crucial area. In particular, the study of electronic images and information in the service options of operating systems enables a clear description of the main facts of criminal offenses, identification of individuals, description of methods and ways of committing a crime, and assessment of the damage caused (Greiman, 2022). This can also be particularly important for confirming and refuting other versions of events. However, it should also be noted that collecting electronic evidence is essential and a complex process that may encounter several challenges. This may include regulating specialist participation, providing appropriate technical support for investigators, ensuring the reliability of the information received, and verifying the accuracy of data obtained from the Internet.

DISCUSSIONS

The main research problem, namely a detailed study of the judicial practice of responding to cybercrimes in Ukraine, determined that cybercrime is one of the key problems in the law enforcement field, which worries modern developed countries, including Ukraine. Such increased interest in cybercrime is not accidental, but instead caused by the prevalence of criminal offenses of this type. In particular, the results showed that the number of cybercrime cases registered in Ukraine increased during the full-scale invasion of Ukraine. In the period from 2022, phishing became especially popular, with more than half of all cases of this type of crime being recorded. This finding aligns with other studies that indicate phishing is a common trend in cybercrime, necessitating serious legal action (Sarkar & Shukla, 2024). Therefore, the increasing trends in the number of cybercrime cases detected have led to an increased interest in the international scientific community in studying the problems of cybercrime and its main directions of combating.

The proposed results also indicate that the activities of cyber fraudsters have undergone significant changes since the beginning of the full-scale invasion by Russian troops. If, in 2017, prominent cases involved the extortion of funds through online delivery and order tools, then, in 2022, phishing would have become the primary type of digital crime. Such results are also confirmed by the findings of other researchers, who have shown that criminals have shifted from direct interaction with a potential victim to acquiring her data using digital tools (Chaika et al., 2024). Scientists believe this process is also connected to a financial component, as many Ukrainian citizens receive payments from European humanitarian aid funds, higher salaries during martial law conditions, and so on. Along with a generally poor digital culture, this makes them vulnerable to cyber manipulation (Reva & Demchenko, 2024). At the same time, the legal regulatory mechanisms for cybercrime prevention are extremely weak: it is almost impossible for phishing victims to prove their innocence in court, as they cannot confirm that the actions taken with their accounts and registries did not occur against their will.

The analysis of the judicial practice of responding to cybercrimes in Ukraine shows that cases related to cybercrimes have several characteristic features, in particular: they are of a transnational type, because, as practice shows, criminals can often operate on the Internet from different parts of the world, and victims or affected persons may be in another country. In Ukrainian reality, access to documents and the belongings of suspects is carried out in accordance with Article 159 of the Criminal Procedure Code of Ukraine (Law of Ukraine No. 912-IX, 2020). Another feature of the criminal cases in Ukraine is that almost all are related to financial fraud. Such results are confirmed by the conclusions of other scientists, which generally indicate the spread of financial fraud in the digital age. The suspects' guilt was proven in local and national courts, after which a warrant was issued. Researchers recognise such a mechanism as quite effective and efficient, such that it does not require the introduction of supranational judicial bodies with new powers (Gallant, 2022). At the same time, it is also worth considering the views of researchers who suggest that digital crimes of the future may be even more complex than financial fraud (Simons et al., 2020). The Ukrainian experience has shown that hacker attacks

organised at the state level by the Kremlin regime are a real threat requiring an international legal assessment. Implementing this process only within the limits of national legislation is impossible.

It is also noted in the proposed results that collecting evidence from electronic systems is a highly relevant aspect of investigating cybercrimes. Cybercrimes are not traceless and leave specific electronic traces. Modern judicial authorities in Ukraine require access to e-mail, correspondence, IP addresses, transactions in electronic payment systems, and other relevant information. The analysed court cases demonstrated that law enforcement officers focused on these details while collecting the necessary evidence. Thus, case law shows the importance of controlling the collection of electronic evidence in cybercrimes. This allows us to effectively investigate such cases without violating the rights of citizens. Such results confirm the researchers' conclusions that the collection of evidence in the field of cybercrimes requires excellent care and professional involvement of specialists (Muliarevych, 2024; Vitvitskiy et al., 2021). At the same time, technologies are constantly improving, so the researchers' view is correct that the legal framework that regulates access to obtaining appropriate evidence should also be updated periodically (Pasupuleti, 2024). As scientists point out, such experiences are already being actively implemented in other countries (Sysoiev et al., 2024). Therefore, in Ukrainian realities, it is also worthwhile to review separate approaches to the legal framework and the mechanisms for its implementation. This makes it possible to confirm the hypothesis that only an integrated approach (legislative, technical, and organisational measures) can ensure an adequate level of cyber protection in the modern world. In the Ukrainian reality, it is necessary to implement numerous measures to achieve lasting positive dynamics.

At the same time, it is necessary to consider certain limitations of the methodology used in the study, which may affect the further interpretation of the obtained results and their scientific significance. First, the selection of necessary scientific literature had certain limits. Emphasis on English-language scientific texts published in professional, peer-reviewed publications has advantages, as such articles have undergone the necessary peer review and preliminary discussion. However, there is a possibility that some relevant opinions published in non-English-language articles were not considered in the obtained results. This aspect must be considered when applying the results found in the article.

CONCLUSIONS

The purpose of this study is to analyze the legal regulation of cyberattacks and cybercrimes in Ukraine, drawing on judicial practice and international experience. Summarizing the results, in the context of active digitalization and the war in Ukraine, the number of cybercrimes has increased significantly, with more than half of them being phishing attacks, and the majority being of a financial and fraudulent nature. The analysis of judicial practice showed difficulties in qualifying cybercrimes, collecting and evaluating electronic evidence, and also identified the need for more precise procedural regulation. The data obtained showed that modern legal mechanisms are not yet fully adapted to the dynamics of digital threats. It was determined that collecting evidence from electronic systems is a crucial part of investigating cybercrimes. Judicial authorities will need access to email, correspondence, IP addresses, transactions in electronic payment systems, and other relevant information. The court cases studied suggest a need to regulate the collection of electronic evidence in cybercrime cases. As innovative technologies continue to improve, it is essential to consider this development when refining the legal framework and creating new bylaws and guidelines that will shape the principles of countering cybercrimes in the future. Therefore, applying complex legislative, technical, and organisational solutions will make it possible to ensure the appropriate level of cyber protection.

The unique contribution of this work lies in the combination of Ukrainian judicial practice analysis with international approaches, which enabled us to identify both the general features of cybercrime and the specific problems inherent in Ukraine. Additionally, a quantitative analysis of the main types of cybercrimes was conducted, enabling us to identify trends in their development more accurately. The theoretical significance of the study lies in the development of a systemic vision of the problems of legal regulation of cybercrime in both global and national contexts. The practical significance lies in the possibility of using the results obtained to enhance law enforcement activities, improve the organization of the judicial process, and strengthen digital security in Ukraine.

A limitation of the study is its focus on the Ukrainian legal field and the analysis of selected court decisions, which do not cover the full range of cybercrimes. Moreover, the selection of necessary scientific literature had certain limits. Emphasis on English-language scientific texts published in professional, peer-reviewed publications has advantages, as such articles have undergone the necessary peer review and preliminary discussion. The prospects for future research lie in expanding the analysis to other countries, comparing the features of national legal systems, as well as in a more detailed study of the effectiveness of international cooperation mechanisms in the field of cybersecurity.

Author Contributions: Conceptualization, V.W., V.H., O.K., D.D. and V.V.; Methodology, V.W., V.H., O.K., D.D. and V.V.; Software, V.W.; Validation, V.W., V.H., O.K., D.D. and V.V.; Formal Analysis, V.W., V.H., O.K., D.D. and V.V.; Investigation, V.W., V.H., O.K., D.D. and V.V.; Resources, V.W., V.H., O.K., D.D. and V.V.; Data Curation, V.W., V.H., O.K., D.D. and V.V.; Writing – Original Draft Preparation, V.W., V.H., O.K, D.D. and V.V.; Writing – Review & Editing, V.W., V.H.,, O.K., D.D. and V.V.; Visualization, V.W.; Supervision, V.W.; Project Administration, V.W.; Funding Acquisition, V.W., V.H., O.K., D.D. and V.V. Authors have read and agreed to the published version of the manuscript.

Institutional Review Board Statement: Ethical review and approval were waived for this study, due to that the research does not deal with vulnerable groups or sensitive issues.

Funding: The authors received no direct funding for this research.

Acknowledgments: The authors have no acknowledgments to declare.

Informed Consent Statement: Informed consent was obtained from all subjects involved in the study.

Data Availability Statement: The data presented in this study are available on request from the corresponding author. The data are not publicly available due to restrictions.

Conflicts of Interest: The authors declare no conflict of interest.

REFERENCES

Ahmad, N., Rahim, F., & Aziz, N. (2024). Can international humanitarian law regulate recent drone strikes?: A case study. *Journal of East Asia and International Law, 17*(1), 159–180. https://doi.org/10.14330/jeail.2024.17.1.09

Alexandrou, A. (2021). *Cybercrime and information technology: Theory and practice: The computer network infrastructure and computer security, cybersecurity laws, Internet of Things (IoT), and mobile devices* (1st ed.). CRC Press. https://doi.org/10.4324/9780429318726

Artemchuk, M., Marukhlenko, O., Sokrovolska, N., Mazur, H., & Riznyk, D. (2024). The impact of economic recession on the financial support of state functions during crisis situations. *Theoretical and Practical Research in Economic Fields, 15*(2), 350. https://doi.org/10.14505/tpref.v15.2(30).15

Baranovska, T. (2024). The impact of cybercrime on state and institutional security: Analysis of threats and potential protection measures. *Economic Affairs, 69*(1s). https://doi.org/10.46852/0424-2513.1.2024.5

Batrachenko, T., Lehan, I., Kuchmenko, V., Kovalchuk, V., & Mazurenko, O. (2024). Cybercrime in the context of the digital age: Analysis of threats, legal challenges and strategies. *Multidisciplinary Science Journal, 6*, 2024ss0212. https://doi.org/10.31893/multiscience.2024ss0212

Borysenko, O., Marukhovska-Kartunova, O., Volkova, V., Baran, A., & Maraieva, U. (2024). The influence of social networks on the formation of modern culture and its relationship with philosophy. *Futurity Philosophy, 3*(3), 80–94. https://doi.org/10.57125/FP.2024.09.30.05

Buçaj, E., & Idrizaj, K. (2024). The need for cybercrime regulation on a global scale by the international law and cyber convention. *Multidisciplinary Reviews, 8*(1), 2025024. https://doi.org/10.31893/multirev.2025024

Chaika, O., Sharmanova, N., & Makaruk, O. (2024). Revitalising endangered languages: Challenges, successes, and cultural implications. *Futurity of Social Sciences, 2*(2), 38–61. https://doi.org/10.57125/FS.2024.06.20.03

Cherniavskyi, S., Babanina, V., Mykytchyk, O., & Mostepaniuk, L. (2021). Measures to combat cybercrime: Analysis of international and Ukrainian experience. *Cuestiones Políticas, 39*(69), 115–132. https://doi.org/10.46398/cuestpol.3969.06

Danidou, Y. (2020). Trusted computing initiative on the spectrum of EU cyber-security legal framework. In T.-E. Synodinou, P. Jougleux, C. Markou, & T. Prastitou (Eds.), *EU Internet law in the digital era* (pp. 277–296). Springer International Publishing. https://doi.org/10.1007/978-3-030-25579-4_13

Despotović, A., Parmaković, A., & Miljković, M. (2023). Cybercrime and cybersecurity in fintech. In S. Benković, A. Labus, & M. Milosavljević (Eds.), *Digital transformation of the financial industry* (pp. 255–272). Springer International Publishing. https://doi.org/10.1007/978-3-031-23269-5_15

Dragojlović, J. (2023). Jurisdiction for criminal offenses of cybercrime: International and national standards. *Pravo - Teorija i Praksa, 40*(suppl), 63–83. https://doi.org/10.5937/ptp2300063D

Erikha, A., & Saptomo, A. (2024). Dilemma of legal policy to address cybercrime in the digital era. *Asian Journal of Social and Humanities, 3*(3), 499–507. https://doi.org/10.59888/ajosh.v3i3.452

Fintech Insider. (2023, November 7). *Cyber fraudsters are becoming more active in Ukraine and the world. What tools do they use and how do they protect themselves?* Retrieved from https://fintechinsider.com.ua/kibershahrayi-stayut-aktyvnishymy-v-ukrayini-ta-sviti-yaki-instrumenty-vony-vykorystovuyut-ta-yak-zahystytysya/

Gajjar, V. R., & Taherdoost, H. (2024). Cybercrime on a global scale: Trends, policies, and cybersecurity strategies. In *2024 5th International Conference on Mobile Computing and Sustainable Informatics (ICMCSI)* (pp. 668–676). IEEE. https://doi.org/10.1109/ICMCSI61536.2024.00105

Gallant, K. S. (2022). The national and international law of criminal jurisdiction: Structure and sources. In *International criminal jurisdiction* (pp. 59–138). Oxford University Press. https://doi.org/10.1093/oso/9780199941476.003.0002

Ghimire, K. (2023). Cyber-attack issues: Laws & policies and the role of librarians. *Access: An International Journal of Nepal Library Association, 2*(01), 216–234. https://doi.org/10.3126/access.v2i01.59002

Greiman, V. A. (2022). Cyber law and regulation. In M. Lehto & P. Neittaanmäki (Eds.), *Cyber security* (pp. 59–78). Springer International Publishing. https://doi.org/10.1007/978-3-030-91293-2_3

Hummelholm, A. (2022). Future smart societies' infrastructures and services in the cyber environments. In M. Lehto & P. Neittaanmäki (Eds.), *Cyber security* (pp. 151–182). Springer International Publishing. https://doi.org/10.1007/978-3-030-91293-2_7

Kagita, M. K., Thilakarathne, N., Gadekallu, T. R., Maddikunta, P. K. R., & Singh, S. (2021). A review on cyber crimes on the Internet of Things. In A. Makkar & N. Kumar (Eds.), *Deep learning for security and privacy preservation in IoT* (pp. 83–98). Springer Singapore. https://doi.org/10.1007/978-981-16-6186-0_4

Kelly, N., & Montasari, R. (2023). Police and cybercrime: Evaluating law enforcement's cyber capacity and capability. In R. Montasari (Ed.), *Applications for artificial intelligence and digital forensics in national security* (pp. 91–103). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-40118-3_6

Kethineni, S. (2020). Cybercrime in India: Laws, regulations, and enforcement mechanisms. In T. J. Holt & A. M. Bossler (Eds.), *The Palgrave handbook of international cybercrime and cyberdeviance* (pp. 305–326). Springer International Publishing. https://doi.org/10.1007/978-3-319-78440-3_7

Khalymon, S., Puzyrov, M., & Prytula, A. (2019). Problems of implementation of whistleblower institution in Ukraine. *Juridical Tribune Journal, 9*(2), 436–454. Retrieved from https://www.tribunajuridica.eu/arhiva/An9v2/11.%20Khalymon,%20Puzyrov,%20Prytula.pdf

Kozlovskyi, S., Kulinich, T., Mazur, H., Khadzhynov, I., & Kozlovskyi, V. (2023). Forecasting the competitiveness of the

agrarian sector of Ukraine in the conditions of war and European integration. *Bulgarian Journal of Agricultural Science, 29*(5), 774–783. Retrieved from https://www.agrojournal.org/29/05-02.pdf

Kravtsov, S., Orobets, K., Shyshpanova, N., Vovchenko, O., & Berezovska-Chmil, O. (2024). Progress and Challenges in Combating Corruption in Ukraine: Pathways Forward. *Journal of Strategic Security*, *17*(2), 28–43. https://doi.org/10.5038/1944-0472.17.2.2223

Kuzior, A., Tiutiunyk, I., Zielińska, A., & Kelemen, R. (2024). Cybersecurity and cybercrime: Current trends and threats. *Journal of International Studies, 17*(2), 220–239. https://doi.org/10.14254/2071-8330.2024/17-2/12

Lavrov, R., Remnova, L., Sadchykova, I., Mazur, H., Tymoshenko, M., Kozlovskyi, V., & Kozlovskyi, S. (2022). Investments in the sustainable development of the potato sector in Ukraine based on the optimal balance of production and consumption. *WSEAS Transactions on Business and Economics, 19*, 186–196. https://doi.org/10.37394/23207.2022.19.19

Law of Ukraine No. 912-IX. (2020). "On the Basic Principles of Cybersecurity in Ukraine". Retrieved from https://zakon.rada.gov.ua/laws/show/2163-19?lang=en#Text

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cybersecurity: Emerging trends and recent developments. *Energy Reports, 7*, 8176–8186. https://doi.org/10.1016/j.egyr.2021.08.126

Mezei, K., & Szentgáli-Tóth, B. (2023). Some comments on the legal regulation on misinformation and cyber attacks conducted through online platforms. *LeXonomica, 15*(1), 33–52. https://doi.org/10.18690/lexonomica.15.1.33-52.2023

Mezzetti, C., Muthukuda, K., & Yuan, H. (2024). Crime in the digital age: Do cyber attacks lead to identity theft? *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4807037

Milon, N. U., Ghose, P., Pinky, T. C., Tabassum, N., Hasan, M. N., & Khatun, M. (2024). An in-depth PRISMA-based review of cybercrime in a developing economy: Examining sector-wide impacts, legal frameworks, and emerging trends in the digital era. *Edelweiss Applied Science and Technology, 8*(4), 2072–2093. https://doi.org/10.55214/25768484.v8i4.1583

Muliarevych, O. (2024). Mitigating input prompt attack vulnerabilities in systems with a language model interface. In *2024 14th International Conference on Dependable Systems, Services and Technologies (DESSERT)* (pp. 1–8). IEEE. https://doi.org/10.1109/dessert65323.2024.11122258

Pasupuleti, M. K. (2024). Legal and regulatory frameworks for AI in cybersecurity: Strategies against threats and fraud. In *AI-enabled security: Defending the digital realm against cyber threats and fraud* (1st ed., pp. 1–18). National Education Services. https://doi.org/10.62311/nesx/97890

Pettoello-Mantovani, C. (2024). Cybercrimes: An emerging category of offenses within the frame of the International Criminal Court jurisdiction. *International Journal of Law and Politics Studies, 6*(2), 06–11. https://doi.org/10.32996/ijlps.2024.6.2.2

Reva, M., & Demchenko, Y. (2024). The role of online psychological testing in a learning process: The Ukrainian case. *E-Learning Innovations Journal, 2*(1), 23–40. https://doi.org/10.57125/ELIJ.2024.03.25.02

Sarkar, G., & Shukla, S. K. (2024). Reconceptualizing online offenses: A framework for distinguishing cybercrime, cyberattacks, and cyberterrorism in the Indian legal context. *Journal of Economic Criminology, 4*, 100063. https://doi.org/10.1016/j.jeconc.2024.100063

Shevchuk, O., Lysodyed, O., Matyukhina, N., Babaieva, O., & Davydenko, S. (2023a). Conflict of interest in the activities of judges in Ukraine and the European Union: A comparative legal study. *Juridical Tribune, 13*(2). https://doi.org/10.24818/TBJ/2023/13/2.06

Shevchuk, O. M., Protsiuk, I. V., Samoshchenko, I. V., Panova, A. V., & Shaposhnyk, A. O. (2023b). The rights to access to information and national security in Ukraine in the system of human rights. *Revista Jurídica Portucalense, 34*, 257–282. https://doi.org/10.34625/issn.2183-2705(34)2023.ic-13

Simons, G., Danyk, Y., & Maliarchuk, T. (2020). Hybrid war and cyber-attacks: Creating legal and operational dilemmas. *Global Change, Peace & Security, 32*(3), 337–342. https://doi.org/10.1080/14781158.2020.1732899

Snail ka Mtuze, S., & Musoni, M. (2023). An overview of cybercrime law in South Africa. *International Cybersecurity Law Review, 4*(3), 299–323. https://doi.org/10.1365/s43439-023-00089-8

Spassova, S. (2023). Disruptions of satellite communication: Comparing cyber attacks and harmful interference for the purposes of legal regulation. In *Space law in a networked world* (pp. 131–142). Brill | Nijhoff. https://doi.org/10.1163/9789004527270_006

Sysoiev, D., Pidbereznykh, I., Mazur, H., Tellis, S., & Vandin, Y. (2024). Administrative law mechanisms for preventing and countering corruption in the field of territorial defence. *Sapienza: International Journal of Interdisciplinary Studies, 5*(4), e24069. https://doi.org/10.51798/sijis.v5i4.859

Tumalavičius, V. (2022). Legal challenges for blockchain projects and cryptocurrencies in the context of sustainable development: International virtual currency market and technology dynamics. *Law, Business and Sustainability Herald, 2*(3), 27–41. Retrieved from https://lbsherald.org/index.php/journal/article/view/55

Unified Register of Court Decisions. (2024). *Search results in the Unified Register of Court Decisions (EUDRSR)*. Retrieved from https://court.opendatabot.ua/search?text=кіберзлочин&adjudication_date_year=2

Verma, A., & Shri, C. (2022). Cyber security: A review of cyber crimes, security challenges and measures to control. *Vision: The Journal of Business Perspective*. Advance online publication. https://doi.org/10.1177/09722629221074760

Vitvitskiy, S., Kurakin, O., Pokataev, P., Skriabin, O., & Sanakoiev, D. (2021). Formation of a new paradigm of anti-money laundering: The experience of Ukraine. *Problems and Perspectives in Management, 19*(1), 354–

363. https://doi.org/10.21511/ppm.19(1).2021.30
Watters, P. A. (2023). *Cybercrime and cybersecurity* (1st ed.). CRC Press. https://doi.org/10.1201/9781003406730
Wessel, R. A., & Heim, T. N. (2023). The various dimensions of cyberthreats: (In)consistencies in the global regulation of cybersecurity. *Anales de Derecho, 40*, 40–65. https://doi.org/10.6018/analesderecho.546921

Publisher's Note: CRIBFB stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.