Journal of Information Systems Engineering and Management
2025, 10(10s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Examining Ukraine's Approaches and Obstacles in Addressing Cyber-Financial Fraud Amid Armed Conflict

Oleg Reznik[a]*, Roman Samsin[b], Liudmyla Nikolenko[c], Iryna Butyrska[d] , Iryna Kozakova[e]
[a] *Department of Economic Cybernetics, Academic and Research Institute of Business, Economics and Management, Sumy State University, Sumy 40000, Ukraine*
[b] *Department of Constitutional, Administrative and Financial Law, Leonid Yuzkov Khmelnytskyi University of Management and Law, Khmelnytskyi 29000, Ukraine*
[c] *Department of Economic and Legal Research Problems of Economic Security, State Organization "V. Mamutov Institute of Economic and Legal Research of the National Academy of Sciences of Ukraine", Kyiv 01032, Ukraine*
[d] *Department of Procedural Law, Yuriy Fedkovych Chernivtsi National University, Chernivtsi 58012, Ukraine*
[e] *Department of Criminal Law, Criminology, Civil Law and Commercial Law, National Academy of Management, Kyiv 03151, Ukraine*

ARTICLE INFO

Received: 14 Oct 2024

Revised: 28 Nov 2024

Accepted: 15 Dec 2024

ABSTRACT

This article provides an in-depth examination of contemporary methods of financial fraud in the digital realm, highlighting strategies for addressing this pervasive issue through the lens of Ukraine's experiences. The authors employ an interdisciplinary methodology that combines methods from legal science, economics, and information technology. Financial fraud is continuously evolving, manifesting in new forms and expanding in scope. Cybercriminals utilize various tactics, including phishing schemes, hacking into banking systems, stealing payment information, and deploying malware to unlawfully access the financial assets of individuals and organizations. Additionally, fraudulent activities are increasingly prevalent on cryptocurrency exchanges, where criminals exploit digital assets. The study underscores that an effective response to financial cybercrime necessitates a holistic approach, which includes monitoring financial transactions to detect anomalous activities, analyzing cyber threats to understand the landscape of financial cybercrime, and enhancing cybersecurity measures to protect against potential threats. Furthermore, user education is emphasized as a critical component, focusing on raising awareness about risks and protective strategies, as many fraudulent activities stem from negligence and a lack of awareness. Throughout the investigation, the authors identify key forms of financial cyber fraud and formulate effective strategies for investigating, preventing, and analyzing these socially harmful acts.

Keywords: Cybersecurity awareness, Fraud prevention strategies, Digital asset security, Cryptocurrency fraud

Introduction

The rapid advancement of modern technologies has given rise to a new category of crime known as cybercrime, which poses significant challenges in the digital landscape (Wall, 2024; Chinedu et al., 2021; Lusthaus, 2024). These crimes, predominantly economic in nature, threaten property relations and disrupt the normal functioning of various economic activities (Homeland Security Digital Library, 2022).

As the fields of criminal law and criminology evolve (Yadav et al., 2023), there is an increasing focus on understanding the concept, characteristics, classifications, and countermeasures related to cybercrime. Financial fraud, a well-established category within criminal law, has undergone a transformation in the context of the 21st-century digital economy (Button & Cross, 2017; Daoud, 2023). The proliferation of automated data processing and communication technologies, coupled with a surge in users engaging with these tools, has created new avenues for criminal exploitation (Halawi & Bacon, 2024; Blythe & Johnson; 2021; Ibrahim, 2022). Consequently, the methods and types of fraud have rapidly evolved, taking on a more virtual form. The utilization of information and communication technologies for illicit purposes has emerged as a pressing challenge for law enforcement and legislative bodies (Abraha, 2021; Leuprech et al., 2023). At the Digital Forum in Seoul, UN Secretary-General Ban Ki-moon highlighted that advancements in information and communication technologies are accompanied by new threats, particularly in the realm of cybercrime (Jansen van Rensburg et al., 2021).

Ukraine's experience in combating cybercrime, especially amid ongoing armed conflict, underscores the urgency of

addressing this issue (Hansel & Silomon, 2023; LB.UA, 2024). The war against Russian Federation has intensified cyber threats (Willett, 2023; Balbaa et al., 2022), with a notable increase in attacks targeting financial systems and fraudulent activities involving bank accounts and cryptocurrencies. This situation necessitates continuous adaptation of countermeasures to effectively address these evolving threats. Given the substantial international support from European Union Nations and the United States, Ukraine has implemented new strategies aimed at monitoring and combating financial fraud in cyberspace. A key focus of these strategies is the protection of banking systems and the prevention of illegal transactions.

This research hypothesizes that the evolving landscape of cybercrime necessitates the development of innovative legal frameworks and enforcement strategies to combat financial fraud in the digital economy effectively.

Objective

The primary objective of this research is to analyze the nature and types of cybercrime, with a specific focus on financial fraud, and to evaluate the effectiveness of current countermeasures in place to combat this issue. To achieve this objective, the research will:

1. Examine the impact of technological advancements on the methods and types of financial fraud.

2. Assess the response of law enforcement agencies to the evolving landscape of cybercrime.

3. Propose recommendations for enhancing legal and operational frameworks to effectively combat cybercrime, particularly financial fraud, in the digital economy.

Conceptual Framework is illustrated in Figure 1.

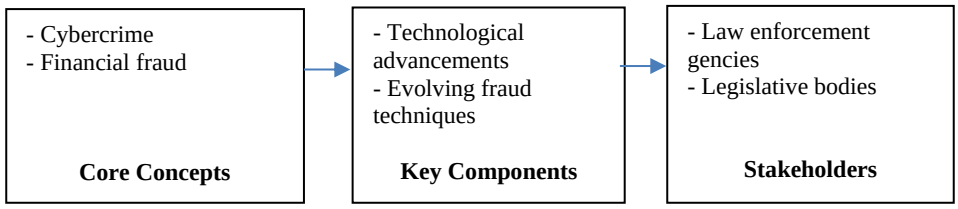

Figure **1** Conceptual Framework

This research aims to analyze the nature and types of cybercrime, particularly financial fraud, and to evaluate the effectiveness of current countermeasures, and suggest improvements to legal and operational strategies to better address these challenges.

Research Methodology

1. Population and Samples

The population for this research consists of online environments where cyber fraud is prevalent, including forums, social media platforms, and messaging applications. Our sample included 523 posts from various online forums and social media groups dedicated to discussions about cyber fraud. This selection was made to ensure a diverse representation of the methods and motivations of cybercriminals. Additionally, we examined statistical data from reputable sources such as the Federal Bureau of Investigation (FBI) and the Internet Crime Complaint Center (IC3) to contextualize the findings within the broader trends of cyber fraud.

2. Research Instrument

We utilized several research methods to achieve our objectives:

Content Analysis: This method enabled us to systematically examine web content associated with specific fraud subtypes, with a particular focus on "phishing." According to the Anti-Phishing Working Group (APWG), phishing attacks increased by 22% in 2022, with over 1.5 million phishing sites reported. By analyzing the language, techniques, and patterns used in these online communications, we gained insights into the strategies employed by cybercriminals.

Comparative Legal Analysis: This approach facilitated the examination of various types of cyber fraud and their evolution, particularly in relation to advancements in information and communication technologies. A report by Cybersecurity Ventures predicts that global cybercrime costs will reach $10.5 trillion annually by 2025, highlighting the urgent need for effective legal frameworks. By comparing different legal frameworks and their responses to cyber fraud, we identified gaps and areas for improvement.

Trend Analysis: We considered current trends in cybercrime, such as the increasing sophistication of social engineering tactics, the utilization of artificial intelligence by cybercriminals, and the role of cryptocurrencies in facilitating illegal transactions.

For instance, a study by Chainalysis revealed that illicit cryptocurrency transactions reached $14 billion in 2021, underscoring the growing intersection of cyber fraud and digital currencies. This analysis provided a comprehensive view of the changing landscape of cyber fraud.

Statistical Analysis: We incorporated statistical data to quantify the impact of cyber fraud. For example, we referenced the FBI's Internet Crime Complaint Center (IC3), which reported a rise in complaints from 791,790 in 2020 to 847,376 in 2021, with financial losses increasing from $4.2 billion to $6.9 billion during the same period. This data helped contextualize the scale and severity of cyber fraud.

3. Collection of Data

Data collection involved a multi-faceted approach. We gathered real-time data from online platforms, forums, and messaging channels known for facilitating illegal activities related to cyber fraud. This included analyzing 523 posts from selected forums and social media groups. Additionally, we collected statistical data from the FBI, IC3, and cybersecurity reports spanning the years 2020 to 2024 to provide a comprehensive overview of the trends and impacts of cyber fraud. The ongoing conflict in Ukraine was also considered, utilizing data from the Office of the Attorney General to assess its influence on cyber fraud patterns (Table 1).

Table 1 Statistical Data on Cyber Fraud (2020-2024)

Year	Total Complaints	Total Financial Losses	Average Loss per Complaint	Percentage Increase in Complaints	Percentage Increase in Losses	Notable Fraud Types Reported	Phishing Complaints	Ransomware Complaints
2020	791,790	$4.2 billion	$5,300			Online shopping fraud, phishing	240,000	2,500
2021	847,376	$6.9 billion	$8,150	7%	64%	Business email compromise, phishing	300,000	3,520
2022	900,000	$8.5 billion	$9,444	6.2%	23.2%	Cryptocurrency fraud, romance scams	350,000	4,000
2023	950,000	$10 billion	$10,526	5.6%	17.6%	Investment scams, tech support fraud	420,000	5,000
2024	1,000,000	$12 billion	$12,000	5.3% (projected)	20% (projected)	Charity scams, identity theft	480,000 (projected)	6,000 (projected)

Source: Compiled by the authors based on data from the Federal Bureau of Investigation (FBI), Internet Crime Complaint Center (IC3), and cybersecurity reports (2020-2024)

4. Data Analysis

Content analysis allowed for the examination of language, techniques, and patterns used in online communications related to cyber fraud. Comparative legal analysis identified gaps in existing legal frameworks. Trend analysis provided insights into the evolving tactics of cybercriminals, while statistical analysis quantified the impact of cyber fraud through reported complaints and financial losses. The findings were contextualized within the framework of the ongoing conflict in Ukraine, highlighting the increase in fraudulent activities in information and telecommunication networks.

Results

In recent years, there has been a growing focus on cyberspace as a domain that wields significant influence over various aspects of social life, including political processes, advertising strategies, economic relations, and international interactions. The year 2020 was particularly pivotal, as the COVID-19 pandemic and the resulting restrictions dramatically transformed daily life for

individuals worldwide. Today, cyberspace is an integral part of modern existence, where an increasing number of actions and decisions take place in the virtual realm (Grigaitytė, 2020). Concurrently, the importance of cybersecurity has escalated, with annual increases in threats related to the protection of confidential information, cyber espionage, sabotage, and fraud. The evolution of cyberspace has been accompanied by a rise in various violations and crimes, exacerbated by the blurring of identities and borders in the digital environment (Financial Conduct Authority, 2024). This situation fosters conditions conducive to anonymity, the dissemination of disinformation, and the execution of cyberattacks, complicating the identification of threat sources and their effective mitigation.

The term "cybercrime" emerged in the 1960s in the United States, marking the beginning of recorded crimes involving computer technologies. With the advent of the Internet in the 1990s, internet fraud expanded significantly. Today, digital technologies are essential to daily life, with critical sectors such as energy, transportation, and finance relying on the stable and secure operation of the Internet (Fissel & Lee, 2023).

As information technologies advance, they not only enhance positive aspects of digitalization but also empower malicious actors to perpetrate cyber fraud. Modern cyberattacks are increasingly sophisticated, employing artificial intelligence, social engineering, and other advanced technologies to bypass security systems. Cybercriminals gain access to confidential data, financial resources, and intellectual property, leading to substantial economic losses and eroding trust in digital systems.

Notably, cyber fraud has emerged as the most frequently committed crime in cyberspace. The COVID-19 pandemic served as a catalyst for the emergence of new fraudulent activities (Ma, 2020). According to the Federal Bureau of Investigation (FBI, 2021), the number of reported cyber fraud complaints reached 791,790, resulting in total financial losses of $4.2 billion. By 2021, complaints had increased to 847,376, reflecting a 7% rise from the previous year, while total financial losses surged to $6.9 billion, marking a 64% increase compared to 2020 (HSDL, 2022). The dynamics of these trends can be attributed to unprecedented changes across various life domains, particularly in work methods, communication, and business practices. This shift has led to a significant increase in digital activity, creating favorable conditions for malicious actors, characterized by factors illustrated in Table 2, Table 2 and Figure 2.

Table 2 Factors Contributing to Cyber Fraud

Factors	**Impact description**
Mass transition to remote work	The shift to remote work due to the pandemic has increased reliance on digital communication tools, creating vulnerabilities in home networks and personal devices.
Increased online activity among the population	With more people engaging in online activities, including shopping and socializing, the number of potential victims has risen significantly.
Rapid digital transformation without adequate security measures	Many organizations rushed to adopt digital solutions without implementing sufficient cybersecurity protocols, leaving systems exposed to attacks.
Growth in the number of potential targets	The expansion of online services and platforms has led to a larger pool of individuals and businesses that can be targeted by cybercriminals.
Simplification of models for committing cyber fraud	Cybercriminals have developed easier and more accessible methods for executing fraud, such as phishing schemes and social engineering tactics, making it simpler for them to deceive victims.

According to McAfee's report, "The Hidden Costs of Cybercrime," global economic losses attributed to cybercrime have reached $1 trillion (McAfee, 2020). Additionally, INTERPOL reported a staggering 569% increase in cyber fraud during the

pandemic (INTERPOL, 2020). From 2022 to 2023, cyber fraud continued to evolve rapidly, adapting to new technological advancements and global events. Key persistent trends include:

1. An increase in phishing attacks, primarily targeting users' financial data.
2. The active development of ransomware attacks, which are increasingly becoming targeted rather than mass attacks.

Cybersecurity experts predict that from 2023 to 2027, fraud in the financial sector will result in losses exceeding $350 billion (AAG, 2024). Data from the European Union Agency for Network and Information Security indicates that fraud constitutes 24% of all criminal offenses in cyberspace, representing nearly a quarter of all offenses analyzed by the agency (CSIRT, 2021).

Table 3 Overview of Cyber Fraud Trends and Statistics (2020–2024)

Year	Complaints	Financial Losses	Percentage Increase in Complaints	Percentage Increase in Losses
2020	791,790	$4.2 billion		
2021	847,376	$6.9 billion	7%	64%
2022	900,000	$8.5 billion	6.2%	23.2%
2023	950,000	$10 billion	5.6%	17.6%
2024	1,000,000	$12 billion	5.3%	20%

Source: Compiled by the authors based on Federal Bureau of Investigation (FBI, 2021) and HSDL (2022), 2022 data – estimated based on trends observed in previous years and projected growth in cyber fraud, 2023 data – estimated based on ongoing trends and expert predictions regarding the rise in cyber fraud, 2024 data – projected based on anticipated growth in digital activities and the increasing sophistication of cybercriminal tactics

The landscape of financial cyber fraud is characterized by its rapid evolution and increasing complexity, driven by technological advancements and changing societal behaviors. Understanding these dynamics is crucial for developing effective countermeasures and enhancing cybersecurity strategies. Figure 2 provides detailed statistics on criminal offenses in cyberspace for 2020-2024 and the share of each within the system of cyber offenses.

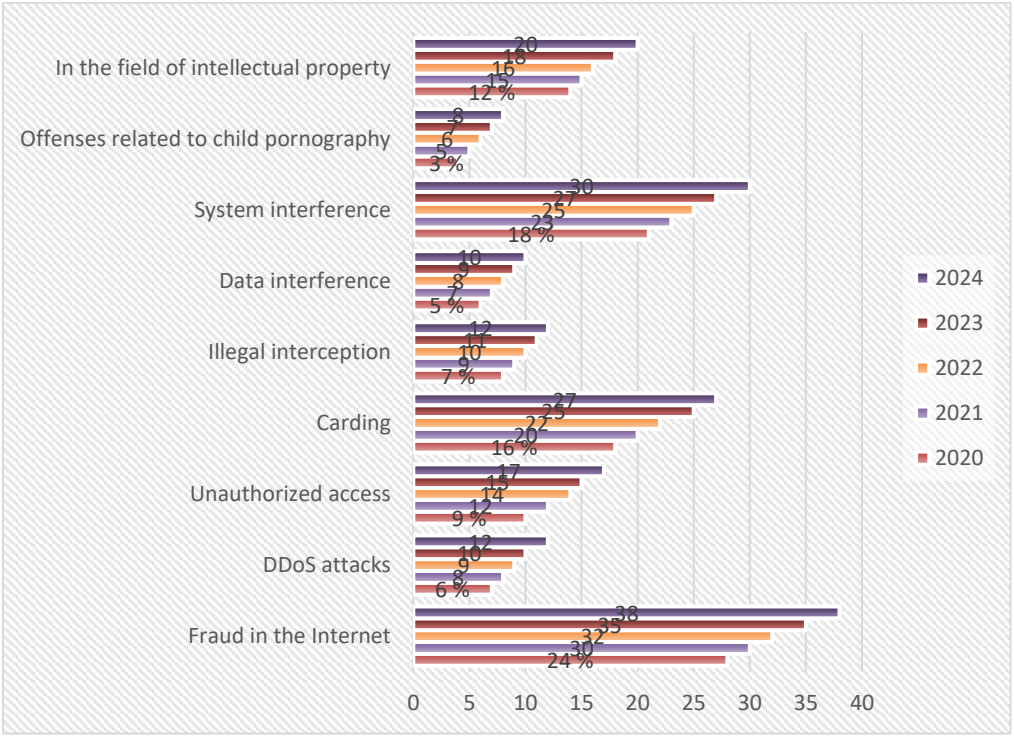

Figure 2 Statistics of Cybercrime Offenses from 2020 to 2024, derived from reports by the European Union Agency for Cybersecurity (ENISA), including their Threat Landscape reports, annual cybersecurity incident reports, and analyses of cybersecurity trends and statistics

Despite advancements in the information sector, cyber fraud continues to be a property crime characterized by deception or breach of trust. Unlike traditional fraud, which typically involves direct interaction with the victim, cyber fraud occurs remotely

through the use of information and communication technologies, such as devices, systems, or networks. The act of deception or breach of trust in the digital realm can take place through various means, including chats, forums, video and audio calls, or through advertisements for non-existent goods and services. There is a wide array of fraudulent schemes in cyberspace, and it is important to recognize that technological advancements significantly contribute to the evolution of these schemes. Matsiakevich (2020) noted the extensive range of fraudulent tactics in the digital environment. He pointed out that the methods of deception or breach of trust are often straightforward and do not necessitate specialized skills or knowledge. Furthermore, the pervasive nature of cyberspace in nearly all aspects of social life creates opportunities for various deceptive practices targeting users.

According to McKinnon (2020), the variety of cyber fraud types is largely attributed to the anonymity afforded by the digital landscape. This anonymity enables individuals committing fraud to easily impersonate others, altering their age, social status, and other identifying features, which can facilitate their deceptive activities. Currently, the most prominent sectors affected by cyber fraud include a) The financial sector (encompassing online banking, auctions, digital wallets, and virtual assets); b) The e-commerce sector (including online stores and various buy-sell listings); c) The entertainment sector (such as online gaming and casinos).

Analysis by the cybersecurity firm CrowdStrike indicates that the e-commerce sector is the primary target of cyber fraud, followed closely by the financial sector. Figure 3 presents statistics on the prevalence of cyber fraud across these different sectors.

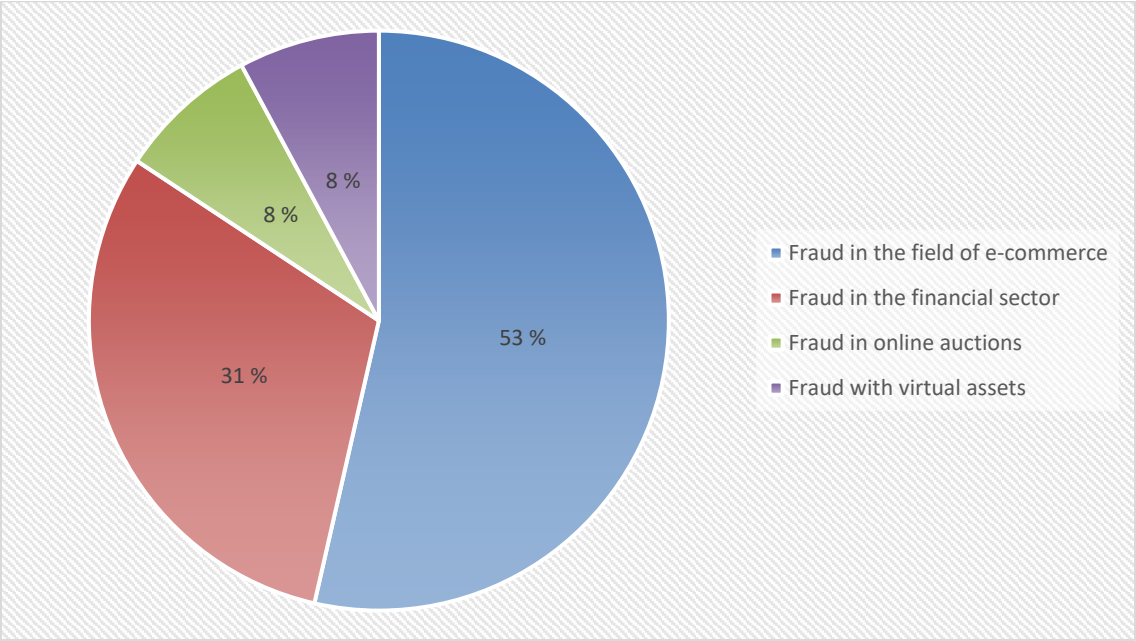

Figure 2. Sectors Affected by Fraudulent Activities in the Digital Realm

We intend to outline the key schemes utilized by fraudsters in their illegal activities, which we have categorized into the following sectors: (i) fraud in the e-commerce sector; (ii) Internet auction fraud; (iii) traditional fraud leveraging information and communication technologies; (iv) fraud in financial services. It is crucial to understand that fraudulent practices in cyberspace are not static; they are constantly evolving to adapt to societal changes. Our selection of these socially harmful acts, characterized by deception or the misuse of trust, is based on their level of social threat, occurrence, and prevalence. Next, we will analyze the distinct types of fraudulent actions present in each sector.

Fraud in the E-commerce Sector

Fraud in the e-commerce sector, often referred to as online trading fraud, is among the most prevalent types of fraudulent schemes. This prominence can be attributed to the relative ease with which such schemes can be executed, requiring minimal specialized skills, and the potential for significant illicit profits (Hasham et al., 2021).

In these fraudulent activities, individuals may take on the role of either sellers or buyers. In the seller scenario, fraudsters create deceptive advertisements for goods or services on various online platforms, including Craigslist, eBay, Amazon, Marketplace, Vinted, and Groupon. The deception lies in the fraudster's intention; they do not plan to deliver the promised goods or services but aim to collect prepayments, often for items that are currently in high demand. For instance, during the pandemic, some fraudsters offered fake services for obtaining vaccination certificates, which were either never delivered or issued without valid certification.

E-commerce platforms have implemented internal cybersecurity measures to mitigate fraudulent activities. One such example is OLX Delivery, which allows buyers to pay only after inspecting their purchases, reserving delivery costs in a conditional account (OLX, 2022). However, despite the availability of such services, only a small fraction of users—approximately 10%—take

advantage of them, leaving many vulnerable to fraud. Fraudsters frequently create counterfeit phishing websites that closely resemble legitimate ones, tricking buyers into depositing funds into fake "guarantee" accounts, believing their money will be transferred to the seller after transaction approval. In reality, the funds go directly to the fraudster's account (RIA Media, 2022).

It is important to note that many of these fraudulent delivery schemes are orchestrated by organized groups, with entire networks dedicated to such illicit activities. Additionally, some fraudsters may not create fake websites but instead gain access to legitimate services, taking a cut from each fraudulent transaction.

The rise of online shopping through social media has also contributed to an increase in fraud within this sector. While some countermeasures exist on traditional marketplaces, platforms like Instagram often leave buyers vulnerable to prepayment scams, as they must pay upfront for goods without adequate protections (Prudka, 2018). In another variant of fraud, the fraudster acts as a buyer, engaging in what is known as "refund fraud." This type of fraud involves a financial transaction initiated after funds have been withdrawn from a cardholder's account, typically when the cardholder refuses to accept or returns the goods. Unlike the seller-focused fraud, refund fraud primarily targets large retailers such as ASOS, Amazon, and Apple. The fraudster acquires goods from these e-commerce entities, pays for them using a credit card or electronic wallet (like PayPal), and then requests a refund while keeping the items. Each retailer has its own refund policies, which can include reasons such as receiving defective items or not receiving the order at all. The success of these schemes often hinges on the fraudster's social engineering skills and the value of the items involved.

One common tactic in the "receiving goods of improper quality" scheme involves intentionally damaging the goods and recording the process to use as evidence for a refund. The fraudster retains the items, which can often be resold after minor repairs. Goldman (2016) identified some prevalent methods of refund fraud related to receiving defective goods, including: 1) filling the parcel with pests or insects; and 2) placing a powder resembling a narcotic substance in the parcel, leading to its disposal. Another popular method is "non-receipt of goods" fraud, where the fraudster claims they did not receive their order. This tactic is effective due to the challenges in proving whether the parcel was delivered. Fraudsters often exploit free shipping services or those with infrequent tracking updates to facilitate this scheme. Consequently, after receiving the goods, the fraudster may contact customer support to request a replacement or a refund for the items they claim they never received (Breen, 2022).

Internet Auction Fraud

A different type of fraud that exploits information and communication technologies is internet auction fraud. In this scheme, fraudsters entice individuals to take part in an auction featuring a purportedly rare item or a product from a specific category, such as numismatics or collectibles. The starting bid for these items is usually set at an attractively low price, creating a sense of urgency and excitement among potential bidders. However, the item itself does not actually exist; in essence, the fraudsters are marketing a non-existent product at a compelling price point. Once a victim wins the auction, the platform automatically deducts funds from their designated card account and deposits them into a guarantee account. These funds are subsequently transferred to the fraudster after the victim's approval, often without the victim realizing they have been deceived (Bulatov, 2015).

A notable variant of internet auction fraud is referred to as the "penny auction." In this scenario, items are listed at an initial price of just 1 to 2 dollars, enticing participants to place minimal bids. However, each bid incurs a fee, which can accumulate quickly, leading participants to lose significant amounts of money without ever receiving the auctioned item. This model preys on the psychology of bidders, who may feel compelled to continue bidding in hopes of winning, ultimately resulting in financial loss without any tangible reward (Queensland Police Service, 2021).

Traditional Fraud Leveraging Information and Communication Technologies

The next area of fraudulent activities we will examine is traditional fraud that employs information and communication technologies. This sector is characterized by the fact that while these socially harmful acts can be considered traditional, their transition into the digital realm amplifies their social danger. Fraud that utilizes telecommunication devices, such as phones, began to gain significant traction in the early 21st century. The rise of social networks, messaging apps, and other online communication tools has further fueled the activities of fraudsters in this domain. Unlike conventional fraud, where the perpetrator meticulously plans one or more socially harmful acts, telephone fraud in cyberspace often targets a large number of individuals, focusing on the volume of potential victims rather than the intricacies of the act itself. The characteristics of distance and the lack of physical interaction between the fraudster and the victim heighten the level of social risk involved. It is important to note that we are considering telephone fraud specifically in the context of criminal offenses that involve direct communication between the victim and the fraudster, with the success of these schemes heavily reliant on the social engineering skills of the perpetrator.

One of the most prevalent schemes among telephone fraudsters is known as "phone scamming." This activity aims to persuade victims to transfer money or disclose personal, employment, banking, or corporate information that the fraudster finds valuable, often for resale to third parties. These scams are typically executed through phone calls or online communication, leveraging social engineering techniques.

In the early 2010s, phone scamming often involved basic deception tactics targeting vulnerable populations, particularly the elderly. A widely used scheme is the "your relative is in trouble" tactic, where fraudsters impersonate doctors or police officers, claiming that a relative is in distress and requires financial assistance to resolve an urgent issue. This method remains effective today. For example, in early August in Vinnytsia, an 82-year-old pensioner was deceived into giving 300,000 hryvnias to a stranger who posed as a doctor, claiming her daughter had been in an accident and needed money for treatment. The perpetrator was later apprehended and identified as a 34-year-old from the Donetsk region, who had a prior conviction for a similar offense (SUSPILNE, 2022).

Another prevalent type of phone scam involves fraudsters posing as bank employees, commonly referred to as the "bank employee" scheme. In this scenario, the fraudster impersonates a bank representative or security officer to extract sensitive information such as bank card details, internet banking passwords, and CVV codes, ultimately leading to the theft of the victim's funds. This type of fraud typically unfolds in several stages, with organized groups often coordinating the efforts. Initially, the fraudster may call the victim, using background information to ask seemingly innocuous questions that build trust. The primary goal at this stage is to ascertain the victim's account balance. In the subsequent phase, the fraudster contacts the victim again, this time posing as a bank security official, and under the guise of protecting the account from potential threats, convinces the victim to withdraw funds and transfer them to a so-called reserve account. Consequently, the victim loses their money (National Police of Ukraine, 2021).

Unlike mass-targeted methods, this targeted approach focuses on specific individuals and involves extended communication with the victim. A current example is the "victims during the war" scheme, where fraudsters claim to have lost their homes and request financial assistance, often attaching fake images and videos to bolster their story. In many cases, fraudsters impersonate military personnel, soliciting funds for fuel, uniforms, or drones. In addition, "fraud shaming" is another subtype of fraud that primarily targets minors, although adults lacking legal awareness can also fall victim. In this scheme, the victim receives a message alleging that they have engaged in criminal activities by visiting prohibited websites or leading an immoral lifestyle. The fraudsters threaten to report these supposed actions to law enforcement, the media, or the victim's acquaintances unless a specified sum of money is transferred. Victims, often misjudging the situation—especially minors fearing repercussions—may comply with the demands to avoid negative consequences.

The final subtype of fraud in this sector involves scam calls from individuals posing as representatives of well-known companies like Microsoft, Dell, or McAfee. These scammers claim that the victim's computer is severely infected with malware that could compromise its functionality, offering to sell software to resolve the issue (Fortinet, 2023).

Fraud in Financial Services

The final area of fraudulent activities we will explore is the financial sector, specifically fraud related to the provision of financial services. One prevalent method of committing fraud in the digital realm is within the lending sector. Numerous financial institutions and banks online offer microcredit services that require only basic identification, such as passport information. In these cases, funds are deposited directly into the client's card accounts. These services have gained significant popularity, particularly among individuals who need financial assistance to purchase a product but prefer not to use traditional credit options. Fraudsters can exploit this system by taking out loans in someone else's name using another person's identification details submitted to the lending institution (Liga Zakon, 2021). It is important to note that this type of fraud does not necessarily require sophisticated software or technical tools, nor does it involve tampering with systems that store, process, or transmit digital information. This fraud can occur both online and through conventional offline methods; the primary distinction lies in how the loan funds are accessed (either as cash or through a card transfer) and the reduced likelihood of direct interaction with employees of the financial institution. This lack of physical contact significantly increases the latency and social risk associated with this method of fraud in cyberspace.

A key aspect of this fraudulent approach is the bank card to which the fraudster directs the loan funds. Often, fraudsters establish a network of "drop bank cards." A "drop" or "money mule" refers to an individual who consents to allow their bank card to serve as a conduit for funds obtained through fraudulent means. The drop facilitates the transfer of illegally acquired money between various accounts. This series of transactions is designed to obscure the trail of the cybercriminals and complicate any subsequent investigations (Cyberpolice, 2017). Frequently, those acting as "drops" are unaware that they are participating in criminal activities.

Discussion

The ongoing military conflict between Ukraine and the Russian Federation has profoundly affected the landscape of cyber fraud, leading to the emergence of new deceptive tactics and exploitation of trust in the digital realm. Since the war began, Ukraine has faced a surge in cyberattacks targeting its energy, financial, communication, and governmental sectors, resulting in increased vulnerability among its citizens to cybercriminal activities. These attacks are designed to destabilize the nation, diminish public morale, and weaken its defense capabilities.

As internet usage expanded in Ukraine and various information and communication technologies evolved, fraudsters began to leverage these advancements as tools for their illicit activities (Levkivska, 2022). The anonymity provided by online interactions makes it easier for cybercriminals to devise schemes aimed at stealing property, funds, and valuables.

It is crucial to recognize the unique characteristics of cyber fraud in the context of martial law, including:

1) All illicit activities in cyberspace are conducted online, making it difficult to identify perpetrators as they utilize digital platforms for their crimes.
2) Fraudulent actions are particularly prevalent during military conflicts, as the chaos creates additional opportunities for fraudsters due to reduced oversight and an increasing number of potential victims.
3) Exploiting the emotional state of the population, fraudsters manipulate feelings of empathy and anger to their advantage.
4) There is a significant misuse of the heightened demand for essential services, such as evacuation from hazardous areas, housing for displaced individuals, and financial assistance programs for internally displaced persons (Herrero et al., 2022).

The conditions of armed aggression from the Russian Federation have exacerbated the emotional vulnerability of the Ukrainian populace. Ongoing stress, fear for personal safety and that of loved ones, uncertainty about the future, and a pervasive sense of danger diminish citizens' psychological resilience, making them more susceptible to the manipulative tactics employed by criminals. Cyber fraudsters are quick to adapt their schemes to the evolving social landscape, taking advantage of current issues related to martial law to enhance the effectiveness of their operations. For example, they may establish fraudulent charitable organizations to solicit donations for victims, offer non-existent evacuation services, or engage in scams involving the sale of scarce essential goods. In doing so, they exploit the emotional fragility and urgent needs of citizens, complicating efforts to combat these fraudulent activities.

Geographically, cyber fraud under martial law has spread across all regions of Ukraine. A notable increase in such offenses correlates with general destabilization, mass population movements, and heightened vulnerability among citizens. According to the Office of the Attorney General, there were 5,842 reported cases of fraud in information and communication networks in 2023, representing a 65% increase from 2022. The situation further deteriorated in 2024, with incidents rising by 44% as of June 1 compared to the previous year (Office of the Attorney General, 2024).

It is important to note that the majority of these crimes are committed by men, who account for approximately 80% of offenders. Their ages range from 21 to 55, with the highest concentration in the 30 to 42 age group. This trend may be attributed to the fact that individuals in this age range possess the life experience, technical skills, and resources necessary to execute complex fraudulent schemes. Although instances of internet fraud involving minors are infrequent, they still raise concerns and highlight the need for enhanced preventive measures targeting young people (National Police of Ukraine, 2024). Women represent about 20% of those engaged in cyber fraud, primarily using social media and online platforms to post fake advertisements for goods or rental properties.

Statistical evidence indicates that major cities such as Kyiv, Lviv, Odesa, and Dnipro are hotspots for increased cyber fraud activity. This trend can be explained by the higher population density, more developed internet infrastructure, and greater digital literacy in these areas. Conversely, border and frontline regions are witnessing a rise in fraud related to evacuation, humanitarian aid, and other urgent needs arising from martial law conditions (SUSPILNE, 2023).

When analyzing the evolution of cyber fraud during martial law, it is essential to consider the primary indicators of fraudulent messages (see Table 3).

Table 3. Warning Signs of Fraudulent Text messages

Ways of Manipulation	Impressions and Reactions	For Case in Point
Urgency	Creates a sense of urgency, pressuring individuals to act quickly without considering consequences	Messages claiming issues with bank accounts or soliciting donations, often appearing to come from trusted sources
Positive Notifications	Elicits positive emotions and promises benefits, prompting immediate action.	Phrases like "You're in luck! This is the price at the old exchange rate," or "Congratulations, you've won!"
Time-Restricted Demands	Imposes specific demands with tight deadlines, creating psychological pressure	Requests to confirm personal information or change passwords within a short timeframe, threatening account suspension
Controlling Fear and Dangers	Utilizes fear tactics to prompt swift action to avoid imagined problems	Messages about potential account suspensions or legal repercussions, often appearing to come from official entities

Abuse of Topical and Social Issues	Takes advantage of current social themes to evoke empathy and prompt action	Fake requests for donations for medical treatment or military support, exploiting the emotional state of the population

These indicators have played a significant role in the development of new schemes, methods, and techniques for perpetrating cyber fraud. We explore several of these in detail as follows.

Fraudulent Fundraising for Military Support

In the context of martial law, one of the most prevalent schemes involves fraudulent fundraising efforts purportedly aimed at supporting the Armed Forces of Ukraine. Scammers create fake social media profiles, websites, and use messaging apps to spread calls for donations. Given the heightened demand for material support for the military during this time of conflict, many citizens, businesses, and members of the diaspora are eager to contribute, particularly for purchasing vehicles, equipment, and ammunition. Unfortunately, this patriotic sentiment is often exploited by fraudsters seeking personal gain. The methods employed in these scams are varied. Fraudsters establish fictitious charitable organizations or funds that exist solely online. They design professional-looking websites and social media pages, utilizing advertising tools to promote their fundraising campaigns. These platforms often feature compelling narratives and images of military personnel or victims, designed to evoke an emotional response from potential donors. Scammers may also impersonate well-known volunteers or organizations, fabricating their details and contact information.

Particularly alarming are instances where fraudsters directly approach business owners and entrepreneurs. They may exploit personal connections or pose as officials from military administrations or state institutions. For example, in the Kyiv region, a group of scammers contacted business owners, claiming to represent military administration leaders and soliciting financial support for the Armed Forces. The ringleader was a foreign national serving a sentence in an occupied territory, and the funds collected were misappropriated, affecting numerous entrepreneurs (SUSPILNE, 2023a). In another case, individuals in the Kharkiv region falsely claimed to represent the Kharkiv Regional Military Administration, spreading misinformation about fundraising efforts for the military (SUSPILNE, 2023a). Currently, on platforms like Telegram and Facebook, nearly one in five posts is related to fundraising for unmanned aerial vehicles, with many of these campaigns turning out to be fraudulent (SUSPILNE, 2023b).

Fraudulent Fundraising for Medical Treatment of Children

Amid the ongoing military conflict and humanitarian crisis in Ukraine, there is an urgent need to assist victims, especially children injured during hostilities. Many individuals and organizations are committed to providing support through donations for medical treatment and rehabilitation. However, this noble cause is often manipulated by fraudsters who create fake volunteer and charitable organizations for their own financial benefit.

The mechanics of this scheme typically involve fraudsters setting up websites, social media profiles, or messaging channels that imitate legitimate charitable organizations. They use professional designs, official language, and recognizable symbols to gain the trust of potential donors. Emotional narratives and images of children affected by the conflict are frequently shared, often accompanied by photographs sourced from public domains or fabricated using technology (Harazd, 2022). The next step involves promoting these campaigns through social media advertising, sometimes collaborating with influencers or employing bots to amplify their reach. To further enhance credibility, they may present forged certificates and licenses of the organizations they claim to represent. Scammers often utilize various crowdfunding methods or target international donors, who may have limited means to verify the authenticity of the information (News Life, 2021). The final phase of this scheme involves using various payment systems to withdraw the illicit funds. Scammers provide convenient options for transferring money, including bank accounts, electronic wallets, and cryptocurrency addresses, making it difficult to trace the financial flows and identify the recipients of the funds.

Fraudulent Claims of International Assistance

In the current climate of martial law and economic uncertainty, many Ukrainians are looking for support from international organizations such as the UN and the European Union. This situation has created opportunities for fraudsters to exploit fake resources to extract personal and financial information from unsuspecting users. The mechanics of this fraudulent activity are relatively straightforward. Scammers create convincing phishing websites that mimic legitimate international organizations, often using similar domain names and offering applications for financial aid, compensation, or social payments. Victims are typically lured to these phishing sites through social media advertisements (National Police of Ukraine, 2023).

Users are prompted to fill out forms requesting personal information, including full names, addresses, phone numbers, identification codes, and bank card details. Once this information is submitted, scammers gain access to sensitive data, which can be used for financial theft or identity fraud (Ukrainian Helsinki Union for Human Rights, 2022).

Fraud Related to Missing or Captured Individuals

The final scheme we will discuss, while not directly linked to martial law, utilizes generative artificial intelligence systems to facilitate the crime. This scheme often involves searching for announcements in messaging apps regarding missing or captured individuals. Criminals reach out to the relatives of these individuals, claiming they can provide information about their whereabouts

for a fee. They often assert that the missing person was injured during combat and is currently receiving medical treatment. This type of fraud preys on the emotional vulnerability of those searching for their loved ones. After receiving payment, the fraudsters typically cease communication, leaving the relatives without any information and suffering both financial losses and emotional distress (UKRINFORM, 2024).

Due to misplaced trust, individuals become more susceptible to deception. Scammers use messages that appear harmless, containing neutral announcements that prompt users to follow links. As a result, many fail to verify the legitimacy of online platforms, neglect to check reviews about products and sellers, and make payments without proper verification. There are numerous instances where individuals do not confirm the authenticity of charitable organizations or the validity of claims made by friends or acquaintances regarding fundraising efforts. Additionally, when renting properties, some people send money in advance based solely on internet photos of the premises (Moroz et al., 2023). This situation underscores the need for innovative and often unconventional approaches to combat organized criminal activities.

It is crucial to implement a cyclical system of preventive measures that begins with addressing the root causes and conditions that lead to socially harmful acts, continues with strategies to prevent and halt such activities, and ultimately returns to addressing the underlying causes and conditions.

Law Enforcement and Criminal Actions to Stop and Fight Online Financial Fraud

Legal measures are essential for addressing one of the key factors contributing to economic cybercrime: the inadequacies in existing legislation. These measures include proposals to enhance laws related to criminal liability for economic offenses and crimes involving computer information, as well as regulations concerning information, communications, and personal data. Legal frameworks are closely intertwined with organizational measures, as they provide the necessary foundation for effective implementation at the legislative level (Akinbowale et al., 2024). Without appropriate legal oversight, many organizational strategies will lack effectiveness. It is important to note that no criminal legislation in any country currently emphasizes the methods used to commit offenses, particularly concerning the role of information and telecommunications technologies as aggravating factors in socially harmful acts. When examining legal strategies for preventing and addressing cyber fraud, it is crucial to focus on international legal initiatives. The lack of clearly defined boundaries in cyberspace poses significant challenges in holding offenders accountable. We believe that international cooperation is the most viable solution to the issue of transnational cybercrime.

Ukraine is increasingly engaged in global efforts to combat cybercrime, especially economic-related offenses. Over the past fifteen years, Ukraine has entered into several agreements aimed at enhancing cooperation in the fight against cybercrime. These agreements facilitate collaborative efforts among nations to tackle computer-related crimes, offenses in the realm of computer information, and cybercrimes, while also focusing on ensuring cybersecurity and safeguarding cyberspace. However, we view these interstate agreements as merely the initial phase in the broader international struggle against cybercrime. At this stage, fundamental rules and principles for counteraction are established, key terms and concepts are defined, and primary strategies for combating these crimes are outlined. The subsequent step should involve the establishment of a Convention under the auspices of the United Nations. We propose that this Convention be divided into two sections. The first section should define cybercrime and cyberspace, along with a comprehensive list of various types of cybercrimes. The second section should outline measures to address the transnational nature of cybercrime, clarify the jurisdiction of states, and lay the groundwork for international collaboration in this area. It is vital that the provisions of this Convention respect the sovereignty of states and their legitimate interests. The measures outlined should prioritize the protection of citizens' rights and freedoms, as any infringement upon these rights is deemed unacceptable.

Another legal approach to countering this detrimental phenomenon involves revising national legislation to align with contemporary digital realities and key cybersecurity strategies. We believe that a successful framework should include the criminalization of certain socially harmful acts that exhibit characteristics of fraud but are not currently classified as crimes due to legislative shortcomings. Additionally, we suggest that the use of information and telecommunications technologies in committing crimes should be recognized as an aggravating circumstance. For effective counteraction against economic crimes in cyberspace and cybercrimes in general, countries should prioritize the development of their National Cybersecurity Strategies. Such strategies should define essential concepts (such as cyberspace and cybercrime) and establish principles for addressing cyber threats, while also outlining the primary governmental actions needed to combat cybercrimes (Table 4).

Table 4 Key Focus Areas of the National Cybersecurity Strategy

Focus Area	Description	Objectives	Key Stakeholders	Implementation Strategies
Protection of Critical Assets	Safeguarding essential sectors such as energy, oil and gas, military, and public services	Ensure the resilience of critical infrastructure against cyber threats	Government agencies, private sector, military	Risk assessments, security audits, and protective measures

Security of Citizens and Organizations	Ensuring the safety of individuals and entities in both computer information and economic activities	Protect personal data and enhance trust in digital services	Citizens, businesses, NGOs	Public awareness campaigns, cybersecurity training programs
Legislative Improvements	Enhancing existing laws to better address cyber threats and crimes	Create a robust legal framework for cybercrime prosecution	Lawmakers, legal experts	Drafting new legislation, amending existing laws, and stakeholder consultations
Addressing Anonymity in Cyberspace	Implementing measures to reduce anonymity that facilitates cybercrime	Increase accountability and traceability in online activities	Law enforcement, internet service providers	Monitoring and regulation of online platforms, user identification protocols
International Cooperation	Fostering collaboration among nations to combat cyber threats effectively	Strengthen global partnerships to share intelligence and resources	International organizations, foreign governments	Bilateral and multilateral agreements, joint training exercises
Development of Specialized Law Enforcement	Establishing dedicated agencies to focus on cybercrime prevention and investigation	Enhance the capacity of law enforcement to tackle cybercrime	Law enforcement agencies, government	Training programs, resource allocation, and establishment of cyber units
Advancement of Information Technologies	Promoting the development and use of secure technologies to protect against cyber threats	Foster innovation in cybersecurity solutions	Tech companies, research institutions	Investment in R&D, public-private partnerships, and technology grants
Enhancing Public Digital Literacy	Increasing awareness and knowledge among the public regarding safe online practices	Empower citizens to protect themselves against cyber threats	Educational institutions, community organizations	Workshops, online courses, and informational resources

Among the informational-criminological measures, a primary focus should be on enhancing cyber hygiene and literacy among the public. These educational initiatives represent a comprehensive approach to eliminating antisocial attitudes within specific groups and fostering a negative perception of cybercriminals. This can include activities through traditional and online media, educational programs in schools and universities, and professional development courses. However, targeted ideological measures will be most effective for specific demographics (Afzal et al., 2024).

Given the decreasing average age of both cybercriminals and their victims, as well as the rising number of juvenile offenders, a highly effective method of ideological influence is to raise awareness about cybercrimes and the associated legal consequences through social media. The widespread use of social networks among minors makes this an essential avenue for effective prevention. With over 75% of children having social media profiles, and many visiting these platforms daily, early education on information security is crucial. Instilling habits such as regularly checking for viruses, installing protective software, and keeping it updated should begin at a young age, similar to teaching children about personal hygiene (Whitty, 2020).

Ukraine's experience in this area is noteworthy, particularly regarding mass notifications to citizens about emerging fraudulent schemes via SMS from cyber police authorities. Each week, the Cyber Police Department of the National Police of Ukraine disseminates information about current cybercrime tactics through mobile operators or messaging apps, advising the public on how to avoid becoming victims (Cyberpolice, 2023b). One of Ukraine's significant achievements in combating cybercrime during the war has been the establishment of the "BRAMA" project, supported by the Cyber Police Department. The "BRAMA" bot serves as an effective tool for preventing and addressing cyber fraud through several key functions: 1) detecting and blocking malicious

websites; 2) allowing users to report suspicious online resources; 3) analyzing reported information to assess its validity and potential threat; 4) blocking confirmed malicious sites to prevent further access and the spread of fraud (Kharkiv Regional Prosecutor's Office, 2024).

Additionally, the bot plays a crucial informational role by keeping citizens informed about current cyber threats. It provides timely updates on new fraudulent schemes, phishing attempts, and other cyber risks, along with recommendations for safe internet practices, personal data protection, and recognizing fraudulent sites. This initiative contributes to raising public awareness and promoting a culture of safe online behavior.

Engaging active users in the fight against cyber fraud is essential, as it encourages them to report suspicious activities and resources. This creates a collaborative platform for sharing experiences and information among users, experts, and law enforcement, thereby enhancing the effectiveness of countering cyber threats. Building an active community fosters quicker and more effective responses to emerging cybersecurity challenges. The bot also supports educational initiatives by distributing learning materials, articles, and videos aimed at improving the public's digital literacy. It informs citizens about webinars, training sessions, and other events where they can learn more about cybersecurity and protective measures against fraud. This is particularly important given the continuous rise in cyber threats and the rapid evolution of technologies used by criminals. As for technical-criminological measures, we advocate for the implementation of specialized mechanisms and methods of information control designed to combat the anonymity associated with economic cybercrimes and to enhance the security of cyberspace itself.

Addressing Anonymous Communication

In our view, addressing the anonymity of users in cyberspace and information networks is a fundamental principle in the fight against economic cybercrime and cybercrime more broadly. The characteristics of modern technology make it challenging to accurately identify who was operating a computer at the time a cybercrime was committed, as users engage indirectly through their accounts. This allows individuals to assert that someone else was using their account to carry out illegal activities. Even when law enforcement identifies an IP address or MAC address associated with a device, the issue of accountability persists, complicating investigations and contributing to a significant amount of unreported crime (Levi et al., 2017).

A promising approach to this challenge is the personalization of internet users. Every individual utilizing the Internet or other information and telecommunications networks should leave a unique identifier. This identifier could take the form of a passport number, electronic signature, facial image, or fingerprint. Among these options, the development and application of biometric technologies, such as facial recognition and fingerprint scanning, stand out as particularly effective in combating anonymity. Most modern computers, laptops, smartphones, and tablets are equipped with built-in cameras capable of recognizing users' faces through specialized software. This software could be integrated into mobile banking applications, for instance. During each transaction, the application could prompt the user to position their face in front of the camera, and if the biometric data matches, the transaction would be authorized. In the future, as this technology becomes more automated, it could also be utilized on social media platforms. This would allow for the recording of biometric data when a fraudster or extortionist interacts with a victim online.

With the widespread adoption of such technology, users in cyberspace would leave undeniable traces of their online activities—specifically, their facial images. One of the key advantages of this approach is that it eliminates intermediaries such as usernames, passwords, internet passports, or physical tokens. The system would automatically identify users based on their biometric information. Additionally, facial recognition technology is already feasible for broad implementation today. We believe that personalizing cyberspace users is the most effective solution to the issue of anonymity, and its realization is primarily a matter of technological advancement.

Conclusion

The increased vulnerability to deception in cyberspace largely stems from individuals' overconfidence in their ability to detect fraud. This misplaced assurance makes them more susceptible to manipulation by scammers, who often use seemingly innocuous messages with neutral advertising content to entice users to click on links. As a result, many fail to verify the legitimacy of online platforms, neglect to research product and seller reviews, and make purchases without additional checks, leading to significant financial losses. Moreover, many individuals do not confirm the legitimacy of charitable organizations or the accuracy of information shared by friends regarding fundraising efforts. This issue is particularly acute during military conflicts, when the number of charitable initiatives rises, and fraudsters exploit the emotional distress of the population. Research shows that about 40% of individuals are willing to donate without verifying information related to aid for war victims (Report Zagoriy Foundation, 2022). To address these challenges, innovative and unconventional strategies are needed to combat organized criminal activities. Comprehensive strategies that integrate legal, social, and technological measures are essential. A cyclical approach to preventive measures—starting with eliminating root causes, followed by prevention and intervention, and concluding with further actions to address underlying issues—will enhance the effectiveness of efforts against cybercrime.

Educational initiatives play a crucial role, as evidenced by a survey from the Institute of Cybersecurity, which found that increasing public awareness of internet fraud can reduce victimization by 35%. Providing timely information about new fraud techniques, the methods used by scammers, and the behavioral traits of fraudsters is vital. Developing instructional materials on recognizing online scams and offering counteraction advice can significantly lower the incidence of such offenses. Research from

the European Cybercrime Centre indicates that comprehensive preventive measures can reduce cybercrime rates by 30% (EU4Digital, 2023).

Suggestion

In the context of martial law, special attention should be given to protecting vulnerable populations who may be more susceptible to fraud due to emotional distress or limited access to reliable information. Collaboration among government agencies, public organizations, and the private sector is essential for establishing an effective system to combat cybercrime.

Acknowledgement

This research is supported by the Ministry of Education and Science of Ukraine and presents findings from project No. 0123U101945, titled “National security of Ukraine through prevention of financial fraud and money laundering: war and post-war challenges.”

Reference

[1] AAG. (2024). *The latest 2024 cyber crime statistics* (updated July 2024). Retrieved from https://aag-it.com/the-latest-cyber-crime-statistics/

[2] Abraha, H. H. (2021). Law enforcement access to electronic evidence across borders: mapping policy approaches and emerging reform initiatives. *International Journal of Law and Information Technology*, 29(2), 118-153.

[3] Afzal, M., Ansari, M. S., Ahmad, N., et al. (2024). Cyber fraud, usage intention, and cybersecurity awareness among e-banking users in India: An integrated model approach. *Journal of Financial Services Marketing*. https://doi.org/10.1057/s41264-024-00279-3

[4] Akinbowale, O., Klingelhöfer, H., Zerihun, M., & Mashigo, P. (2024). Development of a policy and regulatory framework for mitigating cyber fraud in the South African banking industry. *Heliyon*. https://doi.org/10.1016/j.heliyon.2023.e23491

[5] Balbaa, M. E., Eshov, M. P., & Ismailova, N. (2022, December). The Impacts of Russian Ukrainian War on the Global Economy in the frame of digital banking networks and cyber attacks. In *Proceedings of the 6th International Conference on Future Networks & Distributed Systems* (pp. 137-146).

[6] Behind the News (2024). *Another fraudulent collection for the Armed Forces of Ukraine*. Retrieved from https://behindthenews.ua/feiki/inshe/chergoviy-shahrayskiy-zbir-dlya-zsu-683/

[7] Blythe, J. M., & Johnson, S. D. (2021). A systematic review of crime facilitated by the consumer Internet of Things. *Security Journal,* 34, 97-125.

[8] Breen, C. F. (2022). *A large-scale measurement of cybercrime against individuals*. Retrieved from http://surl.li/iavyy

[9] Bulatov, A. S. (2015). Kryminalne manipuliuvannia pid chas shakhraistva [Criminal manipulation during fraud]. *Legal Psychology*. Retrieved from http://surl.li/iavzf

[10] Button, M., & Cross, C. (2017). Technology and Fraud: The ‘Fraudogenic’consequences of the Internet revolution. In *The Routledge handbook of technology, crime and* justice (pp. 78-95). Routledge.

[11] Chinedu, P. U., Nwankwo, W., Masajuwa, F. U., & Imoisi, S. (2021). Cybercrime Detection and Prevention Efforts in the Last Decade: An Overview of the Possibilities of Machine Learning Models. *Review of International Geographical Education Online*, 11(7).

[12] CSIRT. (2021). *2021 report on CSIRT: Law enforcement cooperation*. European Union Agency for Cybersecurity. Retrieved from http://surl.li/iaoas

[13] Cyber Digest. (2024). *Cyber security overview - 2024. Retrieved from https://www.rnbo.gov.ua/files/%D0%9D%D0%9A%D0%A6%D0%9A/Cyber*%20digest_Apr_2024_UA.pdf

[14] Cyberpolice. (2017). *Don't become a drop! - Free cheese can only be found in the mousetrap*. Retrieved from https://www.cyberpolice.gov.ua/article/ne-stavaj-dropom-198/

[15] Cyberpolice. (2023a). *"A parcel for you" – The cyber police warns of a new fraudulent scheme*. Retrieved from https://cyberpolice.gov.ua/article/vam-posylka---kiberpolicziya-poperedzhaye-pro-novu-shaxrajsku-sxemu-3593/

[16] Cyberpolice. (2023b). *How not to become a victim of fraud when selling goods on the Internet: Recommendations of the cyber police*. Retrieved from https://cyberpolice.gov.ua/news/yak-ne-staty-zhertvamy-shaxrajstva-pid-chas-prodazhu-tovariv-v-interneti--rekomendacziyi-kiberpolicziyi-8050/

[17] Daoud, G. (2023). *The Evolving Nature Of Financial Crime With The Increase Of Internet Capabilities. Challenge Identification, Legal Considerations And Policy Recommendations* (Doctoral dissertation, School of Advanced Study).

[18] Decree of the President of Ukraine. (2021). *About Cyber Security Strategy of Ukraine*. Retrieved from https://zakon.rada.gov.ua/laws/show/447/2021#Text

[19] EU4Digital. (2023). *CyberEast - Cyber Crime Action for Cyber Resilience in the Eastern Partnership Region*. Retrieved from https://eufordigital.eu/uk/discover-eu/cybereast-action-on-cybercrime-for-cyber-resilience-in-the-eastern-partnership-region/

[20] Federal Bureau of Investigation. (2021). *FBI releases the Internet Crime Complaint Center 2020 Internet Crime Report, including COVID-19 scam statistics*. Retrieved from https://www.fbi.gov/news/press-releases/fbi-releases-the-internet-crime-complaint-center-2020-internet-crime-report-including-covid-19-scam-statistics

[21] Financial Conduct Authority. (2024). *Financial crime guide: A firm's guide to countering financial crime risks*. Retrieved from https://www.handbook.fca.org.uk/handbook/FCG.pdf

[22] Fissel, E. R., & Lee, J. R. (2023). The cybercrime illusion: Examining the impact of cybercrime misbeliefs on perceptions of cybercrime seriousness. *Journal of Criminology*, 56(2-3), 150-169. https://doi.org/10.1177/26338076231174639

[23] Fortinet. (2023). *What is internet fraud?* Retrieved from https://www.fortinet.com/resources/cyberglossary/internet-fraud

[24] Goldman, Z. K. (2016). *Deterring financially motivated cybercrime: Economic espionage*. Retrieved from http://surl.li/iavym

[25] Grigaitytė, U. (2020). Nusikaltimai virtualioje erdvėje – šiuolaikiniai iššūkiai ir prevencijos galimybės [Crimes in virtual space - modern challenges and prevention opportunities]. *Vilnius University Open Series*. https://doi.org/10.15388/OS.TMP.2020.13

[26] Halawi, L., & Bacon, R. (2024). Exploring the Nexus of Cybercrime, Money Laundering, Ethics and Deterrence in the Age of Smart Machines. *Corruption, Bribery, and Money Laundering - Global Issues*. DOI: 10.5772/intechopen.1004131

[27] Hansel, M., & Silomon, J. (2023). On the peace and security implications of cybercrime: a call for an integrated perspective. *IFSH*, Research Report #012.

[28] Harazd. (2022). *Financial aid fraud and fake payments from scammers*. Retrieved from https://harazd.bank.gov.ua/article/sahrajstvo/scenarii-platiznogo-sahrajstva/sahrajstvo-z-oformlennam-finansovoi-dopomogi-ta-fejkovi-viplati-vid-aferistiv

[29] Hasham, S., Joshi, S., & Mikkelsen, D. (2021). *Financial crime and fraud in the age of cybersecurity: As cybersecurity threats compound the risks of financial crime and fraud, institutions are crossing functional boundaries to enable collaborative resistance*. McKinsey & Company. Retrieved from http://surl.li/iaobj

[30] Herrero, J., Torres, A., Vivas, P., & Urueña, A. (2022). Smartphone addiction, social support, and cybercrime victimization: A discrete survival and growth mixture model. *Psychosocial Intervention*, 31(1), 59-66. https://doi.org/10.5093/pi2022a3

[31] Homeland Security Digital Library. (2022). *2021 Internet crime report*. Retrieved from https://www.hsdl.org/c/2021-internet-crime-report/

[32] Ibrahim, H. (2022). A Review on the Mechanism Mitigating and Eliminating Internet Crimes using Modern Technologies: Mitigating Internet crimes using modern technologies. *Wasit Journal of Computer and Mathematics Science*, 1(3), 50-68.

[33] INTERPOL. (2020). *Cybercrime: COVID-19 impact*. Retrieved from https://www.interpol.int/en/content/download/15526/file/COVID-19%20Cybercrime%20Analysis%20Report-%20August%202020.pdf

[34] Kharkiv Regional Prosecutor's Office. (2024). *Telegram bot BRAMA: Join the fight against disinformation and Russian propaganda*. Retrieved from https://khar.gp.gov.ua/ua/news.html?_m=publications&_t=rec&id=354654&fp=191

[35] LB.UA. (2024). *On behalf of Synegubov, fraudsters sent out fake requests for collection to the Armed Forces*. Retrieved from https://lb.ua/society/2024/05/28/615703_vid_imeni_siniegubova_shahrai.html

[36] Leuprecht, C., Jenkins, C., & Hamilton, R. (2023). Virtual money laundering: policy implications of the proliferation in the illicit use of cryptocurrency. *Journal of Financial Crime*, 30(4), 1036-1054.

[37] Levi, M., Doig, A., Gundur, R., et al. (2017). Cyberfraud and the implications for effective risk-based responses: Themes from UK research. *Crime, Law and Social Change*, 67, 77–96. https://doi.org/10.1007/s10611-016-9648-0

[38] Levkivska, Y. V. (2022). *Vplyv voiennoho stanu na transformuvannia ta rozvytok internet-shakhraistva v Ukraini* [*The influence of martial law on the transformation and development of Internet fraud in Ukraine*]. Retrieved from https://dspace.onua.edu.ua/items/01e3aa71-4478-433e-aae1-f0b228afa00e

[39] Liga Zakon. (2021). *Fraudsters took an online loan in your name: What to do?* Retrieved from https://jurliga.ligazakon.net/news/208174_shakhra-vzyali-na-vashe-mya-onlayn-kredit-shcho-robiti

[40] Lusthaus, J. (2024). Reconsidering Crime and Technology: What Is This Thing We Call Cybercrime?. *Annual Review of Law and Social Science*, 20(1), 369-385.

[41] Ma, K. W. F. (2020). *COVID-19 and cyber fraud: Emerging threats during the pandemic*. Retrieved from https://doi.org/10.13140/RG.2.2.18540.39042

[42] McAfee. (2020). *The hidden costs of cybercrime*. Retrieved from https://companies.mybroadband.co.za/axiz/files/2021/02/eBook-Axiz-McAfee-hidden-costs-of-cybercrime.pdf

[43] Ministry of Digital Transformation of Ukraine. (2023). *Study of digital literacy in Ukraine*. Retrieved from https://osvita.diia.gov.ua/uploads/1/8800-ua_cifrova_gramotnist_naselenna_ukraini_2023.pdf

[44] Moroz, V. P., Chaplinskyi, K. O., Boguslavskyi, M. G., & Voloshina, M. O. (2023). *Protydiia orhanizovanii zlochynnosti v Ukraini: suchasnist ta perspektyvy [Combating organized crime in Ukraine: Modernity and prospects: Monograph*]. Dnipro, UA: Dnipro State University of Internal Affairs (DSUIA).

[45] National Police of Ukraine. (2021*). The police of the Lviv region warn: Be vigilant and do not let fraudsters deceive you*. Retrieved from https://lv.npu.gov.ua/news/politseyski-lvivshchini-zasterigayut-budte-pilnimi-ta-ne-dayte-shakhrayam-oshukati-sebe

[46] National Police of Ukraine. (2023). *Fraudsters appropriate citizens' funds under the pretext of providing financial aid from international organizations*. Retrieved from https://www.npu.gov.ua/news/shakhrai-pryvlasniuiut-koshty-hromadian-pid-pryvodom-nadannia-hroshovoi-dopomohy-vid-mizhnarodnykh-orhanizatsii

[47] *National Police of Ukraine*. (2024). An official web-based platform. Retrieved from https://www.npu.gov.ua/

[48] News Life. (2021). *Collecting money to help dead children: How fake charity funds work in Ukraine*. Retrieved from https://society.novyny.live/sobiraiut-dengi-na-pomoshch-uzhe-umershim-detiam-kak-rabotaiut-feikovye-blagotvoritelnye-fondy-v-ukraine-23204.html

[49] Nikkel, B. (2020). Fintech forensics: Criminal investigation and digital evidence in financial technologies. *Forensic Science International: Digital Investigation*, 33, 200908. https://doi.org/10.1016/j.fsidi.2020.200908

[50] Office of the Attorney General. (2024). *Statistics of criminal illegality*. Retrieved from https://erdr-map.gp.gov.ua/csp/map/index.html#/table

[51] OLX. (2022). *What is the OLX Delivery service?* Retrieved from http://surl.li/ovqo

[52] Prudka, L. M. (2018). Psykholohichni osoblyvosti shakhraistva v merezhi Internet [Psychological features of fraud in the Internet]. *Southern Ukrainian Legal Journal*. Retrieved from http://www.sulj.oduvs.od.ua/archive/2018/2/10.pdf

[53] Queensland Police Service. (2021). *Internet auction fraud*. Retrieved from https://www.police.qld.gov.au/safety-and-preventing-crime/r-u-in-control/internet-auction-fraud

[54] Report Zagoriy Foundation. (2022). *Charity in times of war*. Retrieved from https://zagoriy.foundation/wp-content/uploads/2022/08/doslidzhennya-2022-1.pdf

[55] RIA Media (2022). *How not to lose money in OLX: The most popular scheme of fraudulent buyers*. 20minut.ua. Retrieved from https://te.20minut.ua/Groshi/yak-ne-vletiti-na-groshi-v-olx-naypopulyarnisha-shema-shahrayiv-pokupt-11296224.html

[56] SUSPILNE. (2022). *Your relative got into an accident: The police told about the most common fraud schemes*. Retrieved from http://surl.li/iavzr

[57] SUSPILNE. (2023a). *He deceived more than 30 citizens under the guise of assistance for the Armed Forces: A fraudster was convicted in Kyiv*. Retrieved from https://suspilne.media/kyiv/563385-pid-vigladom-dopomogi-dla-zsu-osukav-ponad-30-gromadan-u-kievi-zasudili-sahraa/

[58] SUSPILNE. (2023b). *In the Kyiv region, the number of cyber frauds has tripled: The prosecutor's office*. Retrieved from https://suspilne.media/kyiv/629658-na-kiivsini-vtrici-zbilsilas-kilkist-kibersahrajstv-prokuratura/

[59] Ukrainian Helsinki Union for Human Rights. (2022). *Financial assistance from international organizations: How not to get caught by fraudsters*. Retrieved from https://www.helsinki.org.ua/articles/hroshova-dopomoha-vid-mizhnarodnykh-orhanizatsiy-iak-ne-natrapyty-na-hachok-shakhraiv/

[60] UKRINFORM. (2024). *Relatives of prisoners and missing persons were given advice on how to protect themselves from fraudsters*. Retrieved from https://www.ukrinform.ua/rubric-society/3894960-rodicam-polonenih-i-zniklih-bezvisti-dali-poradi-ak-ubezpecitisa-vil-sahraiv.html

[61] Van Rensburg, S. J., Viviers, W., Parry, A., Strydom, P. D. F., Kühn, M.-L., Orkoh, E., Grater, S., Hoffman, A., & Joubert, B. (2021). *Africa's digital future: From theory to action* (p. 420). AOSIS.

[62] Wall, D. S. (2024). *Cybercrime: The transformation of crime in the information age*. John Wiley & Sons.

[63] Whitty, M. T. (2020). Is there a scam for everyone? Psychologically profiling cyberscam victims. *European Journal of Criminal Policy Research*, 26, 399–409. https://doi.org/10.1007/s10610-020-09458-z

[64] Willett, M. (2023). The cyber dimension of the Russia–Ukraine War. In Survival: October-November 2022 (pp. 7-26). Routledge., M. (2023). The cyber dimension of the Russia–Ukraine War. In *Survival: October-November 2022* (pp. 7-26). Routledge.

[65] Yadav, S., Yadav, S., Verma, P., Ojha, S., & Mishra, S. (2023). Artificial Intelligence: An Advanced Evolution In Forensic and Criminal Investigation. *Current Forensic Science*, 1(1), e190822207706.