Library Progress International *Print version ISSN 0970 1052*
Vol.44 No.3, Jul-Dec 2024: P. 21444-21457 *Online version ISSN 2320 317X*

Original Article *Available online at www.bpasjournals.com*

Strategies and Challenges of Combating Cyber-Financial Fraud: An Analysis of Ukraine's Experience During the Military Conflict

Oleg Reznik[1], Roman Samsin[2], Liudmyla Nikolenko[3], Iryna Butyrska[4], Kozakova Iryna[5]

[1]Department of Economic Cybernetics, Academic and Research Institute of Business, Economics and Management, Sumy State University, Sumy – 40000, Ukraine. E-mail: reznikoleg07@gmail.com
[2]Department of Constitutional, Administrative and Financial Law, Leonid Yuzkov Khmelnytskyi University of Management and Law, Khmelnytskyi – 29000, Ukraine. E-mail: Kondvaleriy54@gmail.com
[3]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. E-mail: ludmilanik13@gmail.com
[4]Department of Procedural Law, Yuriy Fedkovych Chernivtsi National University, Chernivtsi – 58012, Ukraine. E-mail: i.butyrska@gmail.com
[5]Department of Criminal Law, Criminology, Civil Law and Commercial Law, National Academy of Management, Kyiv – 03151, Ukraine. E-mail: irakozakova4@gmail.com

How to cite this article: Oleg Reznik, Roman Samsin, Liudmyla Nikolenko, Iryna Butyrska, Kozakova Iryna (2024) Strategies and Challenges of Combating Cyber-Financial Fraud: An Analysis of Ukraine's Experience During the Military Conflict. *Library Progress International,* 44(3), 21444-21457.

ABSTRACT
The article is dedicated to a detailed analysis of modern methods of financial fraud in cyberspace, substantiating the prospects for combating this destructive phenomenon based on Ukraine's experience. In this study, the authors employed an interdisciplinary approach, combining methods from legal science, economics, and information technology. Financial fraud is constantly evolving, taking on new forms and scales. Cybercriminals actively utilize various methods such as phishing attacks, hacking banking systems, stealing payment data, and deploying malicious software to gain unauthorized access to the financial resources of individuals and organizations. Simultaneously, illegal activities are increasingly spreading on cryptocurrency exchanges, where fraudsters manipulate digital assets. It is emphasized that effective counteraction to financial cybercrime requires a comprehensive approach. This includes monitoring financial transactions to detect anomalous activity, analyzing cyber threats, and enhancing cybersecurity measures. It is also crucial to educate users about potential threats and ways to protect personal data, as the majority of fraudulent schemes are executed through negligence and lack of knowledge. During the course of the investigation, the authors identified the main forms of financial cyber fraud and developed effective methodologies for investigating, preventing, and analyzing such socially dangerous acts.

Keywords: *Cybersecurity models, information sources, financial fraud detection, analysis techniques, cryptocurrency manipulation, anomalous transaction monitoring.*

1. Introduction

With the advancement of modern technologies, conditions have emerged for the appearance of a new type of crime committed in cyberspace—cybercrimes. Most of them are economic in nature and are capable of causing real harm to property relations and the normal functioning of entrepreneurial or other economic activities (Homeland Security Digital Library, 2022). In the science of criminal law and criminology, issues concerning the concept, nature, types of cybercrimes, and measures to counteract them are actively discussed.

Financial fraud belongs to the traditional categories of crimes well-studied in criminal law. However, the formation of the "digital economy" in the 21st century, along with the reduction in the cost of automated data processing and transmission means and the rapid growth in the number of users of modern computer technologies, has opened new opportunities for the criminal world. As a result, the types and methods of fraud are quickly and significantly transforming, acquiring an increasingly virtual dimension.

The use of information and telecommunication technologies for criminal purposes in recent years has become a serious challenge for both law enforcement agencies and legislators. At the Digital Forum in Seoul, UN Secretary-General Ban Ki-moon noted that the revolution in the field of information and communication technologies is accompanied by new threats associated with cybercrime.

Ukraine has significant experience in countering cybercrime, especially under conditions of armed conflict (LB.UA, 2024). During the war against Russia, cyber threats became one of the key challenges for Ukrainian law enforcement agencies. Attacks on financial systems and the use of cyberspace for fraud with bank accounts and cryptocurrencies have significantly increased, requiring constant updates of countermeasures.

Due to significant international support, particularly from European Union countries and the USA, Ukraine has adopted new strategies for monitoring and combating financial fraud in cyberspace. Special emphasis is placed on protecting banking systems and preventing illegal transactions.

2. Methodology

In conducting this research, we employed an interdisciplinary approach that combines methods from legal science, economics, and information technology. It is worth noting that numerous scholarly works are dedicated to characterizing cyber fraud, its role in the sphere of cybercrime, and ways to counteract this socially dangerous phenomenon.

These works contain a range of proposals, particularly concerning the counteraction of the latest types of cyber fraud in the activities of law enforcement agencies, financial institutions, and cybersecurity organizations. However, they are mostly substantiated at a theoretical level and do not take into account the newest cyber threats, techniques, and methods used by cybercriminals when committing such socially hazardous acts.

We, on the other hand, applied a different approach, which involves analyzing websites, forums, and messenger channels that specialize in illegal activities, particularly cyber fraud. Using modern scientific cognition methods, we analyzed the ways and schemes of committing cybercrimes through deception and abuse of trust, both as auxiliary and primary means of committing a crime.

The content analysis method allowed us to conduct a systematic analysis of web content related to specific subtypes of fraud, particularly "phishing." The comparative legal method enabled us to analyze the main types of cyber fraud and their evolution using elements of information and telecommunication technologies. In addition, we took into account current trends in cybercrime, such as the increasing complexity of social engineering attacks, the use of artificial intelligence by cybercriminals, and the exploitation of cryptocurrencies for illegal transactions. By integrating these latest developments and applying advanced scientific cognition methods, our research provides a deeper understanding of cyber fraud and offers practical recommendations to enhance the effectiveness of cybersecurity measures.

3. Result and Discussion

3.1. General Characteristics of Financial Cyber Fraud: Main Methods of Commission

In recent times, there has been increasing attention to cyberspace as an environment possessing unique tools of influence over various spheres of social life, including political processes, advertising strategies, economic relations, and international interactions. Particularly significant in this context was the year 2020, marked by the pandemic and unprecedented restrictions that substantially altered the way of life for people worldwide.

Today, cyberspace is an integral element of modern reality, where an ever-growing number of actions and decisions occur in the virtual domain (Grigaitytė, 2020). Simultaneously, the relevance of issues related to ensuring cybersecurity is escalating. Each year sees a rise in threats associated with the preservation of confidential information, cyber espionage, sabotage, and fraud. The development of cyberspace is accompanied by an escalation of various violations and crimes, connected to the blurring of identities and borders in the virtual environment (Financial Conduct Authority, 2024). This creates favorable conditions for anonymization, the spread of disinformation, and the execution of cyber attacks, complicating the tracking of threat sources and their effective neutralization.

The term "cybercrime" first appeared in the 1960s in the USA when the initial crimes committed using computer technologies were recorded. With the development of the Internet in the 1990s, the scale of internet fraud significantly increased. Today, digital technologies have become an indispensable part of daily life, and many critically important sectors—such as energy, transport, and finance—depend on the stable and secure operation of the Internet (Fissel & Lee, 2023).

With the advancement of information technologies, not only are the positive aspects of digitalization being enhanced, but so too are the methods used by malicious actors to commit cyber fraud. Modern cyber attacks are becoming increasingly complex, utilizing artificial intelligence, social engineering, and other advanced technologies to circumvent security systems. Malicious actors gain access to confidential data, financial resources, and intellectual property, which can lead to significant economic losses and undermine trust in digital systems.

It is worth noting that in today's world, the most frequently committed crime in cyberspace is cyber fraud. As previously mentioned, the catalyst for the development of new forms of fraudulent activities in cyberspace was the Covid-19 pandemic (Ma, 2020). According to statistical data from the Federal Bureau of Investigation (FBI, 2021), the number of registered complaints about cyber fraud reached 791,790, with total financial losses amounting to $4.2 billion. By 2021, the number of registered complaints had risen to 847,376—a 7% increase compared to 2020—and total financial losses from cyber fraud reached $6.9 billion, marking a 64% increase compared to 2020 (HSDL, 2022).

Such dynamics are primarily explained by unprecedented changes in all spheres of life, particularly in methods

of work, communication, and business conduct. This led to a significant increase in digital activity, which in turn created favorable conditions for malicious actors, including:

a) Mass transition to remote work;
b) Increased online activity among the population;
c) Rapid digital transformation without adequate security measures;
d) An increase in the number of potential targets;
e) Simplification of models for committing cyber fraud.

According to McAfee's report, "The Hidden Costs of Cybercrime," global economic losses from cybercrime have reached $1 trillion (McAfee, 2020). Simultaneously, INTERPOL data indicated a 569% increase in cyber fraud during the pandemic (INTERPOL, 2020). In the period from 2022 to 2023, cyber fraud continued to develop rapidly, adapting to new technological advancements and global events. Among the main trends that, unfortunately, have become persistent are: 1) an increase in phishing attacks, primarily targeting users' financial data; 2) active development of ransomware attacks, which are increasingly becoming targeted rather than mass attacks.

Cybersecurity specialists and analysts predict that from 2023 to 2027, fraud in the financial sector will cause companies losses exceeding $350 billion (AAG, 2024). According to data from the European Union Agency for Network and Information Security, the share of fraud in cyberspace among all committed criminal offenses is 24%.

Notably, this constitutes almost a quarter of all offenses in cyberspace analyzed by the agency (CSIRT, 2021). Figure 1 provides detailed statistics on criminal offences in cyberspace for 2021 and the share of each within the system of cyber offences.

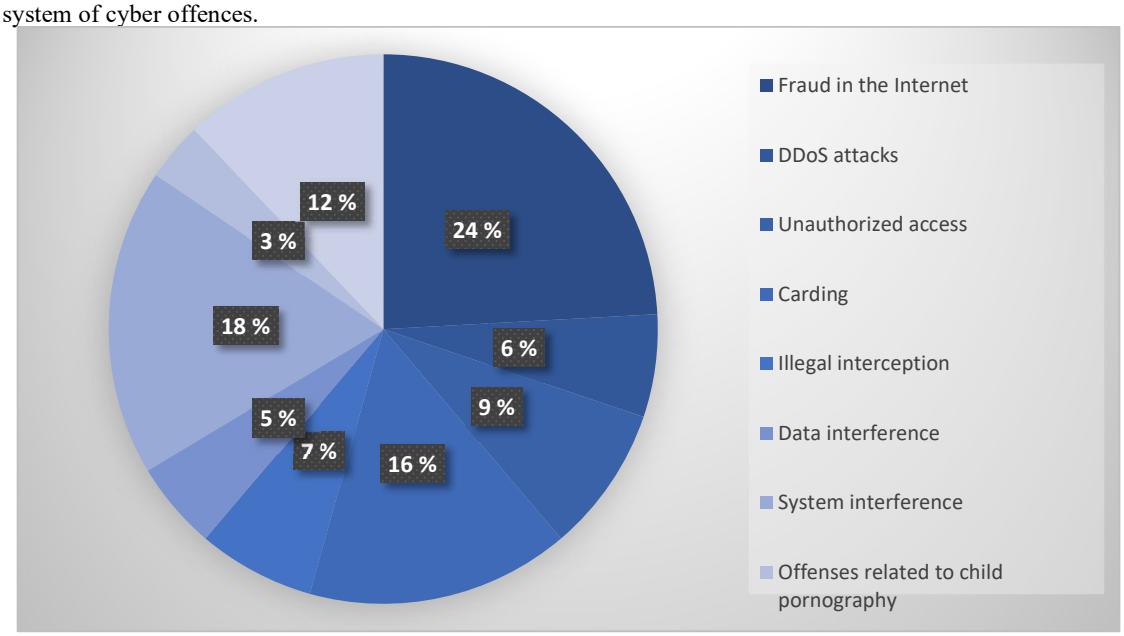

Figure 1. *Statistics of criminal offenses in cyberspace in 2021 according to the data of the European Union Agency for Cybersecurity*

Despite evolutionary processes in the information segment, fraud in cyberspace remains a criminal offense against property, committed through deception or abuse of trust. The main difference from classical fraud is simply that the deception does not occur during direct physical contact with the victim but in a remote form, namely through the use of information and telecommunication technologies (devices, systems, or networks).

The very act of deception or abuse of trust in cyberspace is possible through communication with the victim via various chats, forums, video and audio calls, or the publication of advertisements for the sale or purchase of non-existent goods or the provision of services. Overall, there is a vast number of fraudulent schemes in cyberspace; at the same time, it is worth noting that technological progress directly influences the innovative aspects of these schemes.

Matsiakevich (2020) explained the great variety of fraudulent schemes in cyberspace: firstly, deception or abuse of trust are relatively simple methods of committing criminal offenses and generally do not require special skills or knowledge; secondly, cyberspace itself has already penetrated almost all spheres of social life, thereby creating prerequisites for the existence of various ways to deceive users of the information space. According to McKinnon (2020), the diversity of types of fraud in cyberspace is primarily due to the anonymity of both cyberspace itself and its users. Cyberspace allows a person who has committed a criminal offense to easily impersonate another

individual, altering their real age, social status, and other identification characteristics, thereby gaining advantages when committing fraud.

It should be highlighted that today the most widespread areas of societal activity in cyberspace are as follows:

a) The financial sector (online banking, online auctions, digital wallets, virtual assets);
b) The e-commerce sector (online shops, various buy-sell advertisements);
c) The entertainment sector (online games, online casinos).

According to analysis by the information security company CrowdStrike, cyber fraud is most frequently directed at the e-commerce sector, with the financial sector in second place. Figure 2 illustrates the statistics of different areas of cyber fraud.

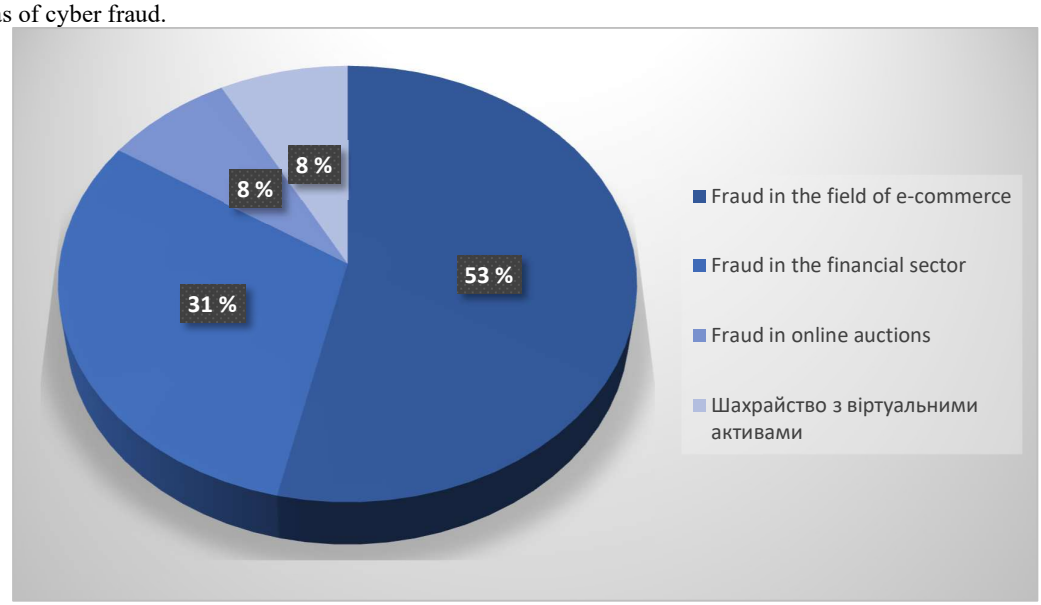

Figure 2. *Areas of Fraudulent Activities in Cyberspace*

We propose to briefly characterize the main schemes used by fraudsters in their illicit activities, which we have divided into sectors, namely:

a) Fraud in the E-commerce Sector;
b) Auction Fraud on the Internet;
c) Traditional Fraud Using Information and Telecommunication Technologies;
d) Fraud in the Provision of Financial Services.

It is important to note that fraudulent schemes in cyberspace are not exhaustive and dynamically change, adapting to society's needs. Our selection of socially dangerous acts committed in the form of deception or abuse of trust was based on their social danger, frequency, and prevalence. We propose to analyze the specific types of fraudulent actions in each sector.

3.2. Fraud in the E-commerce Sector

Fraud in the e-commerce sector, or as it is often called, fraud related to trading—the purchase of goods online—is probably one of the leaders among other fraudulent schemes. This is primarily due to the ease of implementing this scheme, which does not require special skills, and the illicit profit gained by the perpetrator (Hasham et al., 2021).

When executing this fraudulent scheme, the individual can act either as a seller of goods or services or as a buyer. The first variant involves creating fake advertisements for the sale of goods or services on various online marketplaces like Craigslist, eBay, Amazon, Marketplace, Vinted, Groupon, and others. The fakeness of the advertisement lies in the fraudster performing the objective side of this criminal offense in the form of deception. The fraudster initially does not intend to provide the service or send the goods to the buyer; their main task is to receive a prepayment for the goods or services, less often the full amount. Fraudsters mostly deal with goods or services that are in public demand at a specific time. For example, during the pandemic, they offered services for obtaining vaccination certificates, which they either did not send to the required address or issued without a valid certification number.

It is worth noting that e-commerce entities use their internal cybersecurity mechanisms to completely eliminate or reduce fraudulent incidents on their trading platforms. An example of such a service is OLX Delivery, which effectively replaces cash on delivery and eliminates commission fees: the buyer pays for the goods only after inspection and receipt at the post office, and the delivery cost is already reserved in a conditional account within

the OLX Delivery service itself (OLX, 2022).

It should be emphasized that despite this service functioning for several years, only 10% of platform users utilize it, and fraudsters actively exploit this. Very often, sellers create fake, phishing websites that externally completely mimic the original (design, domain, functions, payment systems for cashless purchases) and subsequently send a fake form to the buyer. The buyer deposits their funds into a fake "guarantee" account, confident that they will be transferred to the seller only after the buyer reviews and approves the transaction. But in fact, the victim transfers funds directly to the fraudster's merchant system (20minut.ua, 2022). We want to draw attention to the fact that fraud with delivery services is committed in complicity, by organized groups; there are entire centers engaged in such illegal activities. At the same time, the fraudster may not create a fake web resource or merchant system but gain access to such a service for a certain percentage of each fraudulent transaction, subsequently receiving "clean" funds from the service owner.

The spread of online trading through social networks has simultaneously led to an increase in fraud in this category. While in the first variant there were at least some local countermeasures to this socially dangerous phenomenon by marketplace owners, when purchasing goods through a platform like Instagram, the victim inevitably faces the problem of prepayment for the goods to cover expenses in case of refusal after receipt. Fraudsters operate according to this scheme and achieve their criminal result due to the mass of offers on the market and the corresponding low price for a similar product on the marketplace (Prudka, 2018).

According to the second variant, the fraudster acts as a buyer of a certain product. An example of this type of fraud is "refund fraud." Refund fraud is a credit financial operation carried out after funds have been debited from the cardholder's account, initiated by the enterprise in case the cardholder refuses to receive the goods or returns them.

Unlike the first variant discussed, this type of fraud targets large network enterprises specializing in the sale of goods, such as ASOS, Amazon, Apple, and others. The essence of this type of fraud lies in obtaining goods from an e-commerce entity, paid for in advance with a card or electronic wallet (PayPal), followed by the refund of the paid funds to the fraudster, while the paid goods also remain with the fraudster. Note that each company has its own algorithm for refunding paid goods for certain reasons, such as receiving goods of improper quality, non-receipt of goods, or receiving other goods. It should be emphasized that the implementation of each refund variant directly depends on social engineering skills and the price of the ordered goods.

The implementation of the method "receiving goods of improper quality" involves deliberately causing minor damage to the goods and simultaneously video-recording the process of damage, subsequently using the video as evidence to obtain a refund. Note that the goods also remain with the fraudster and, after minor repairs, are subject to sale.

Goldman (2016) highlighted among the most popular methods of refund fraud related to receiving goods of improper quality: 1) the parcel box contents were filled with pests or insects that spoiled it; 2) the parcel box contents were filled with powder visually similar to a narcotic substance, resulting in the box and contents being discarded.

The method of refund fraud known as "non-receipt of goods" is also popular among fraudsters due to the difficulty of proving whether the fraudster received the parcel. For successful implementation, fraudsters often use free delivery services or services that do not provide or rarely update trackers on the parcel.

As a result, the fraudster receives the ordered goods and then, after some time, contacts customer support demanding a replacement for the goods they "did not receive" or a refund to their card (Breen, 2022).

3.3. Auction Fraud on the Internet

Another type of fraud using information and telecommunication technologies is auction fraud on the internet. Fraudsters offer participation in an auction where the lot is a certain rare item or a product of a specific category, say numismatics. The starting price for such goods is always understated, and the lot itself does not actually exist; that is, fraudsters offer to buy a non-existent item at an attractive price. After the victim wins the auction, the service automatically debits funds from the specified card account to the service's guarantee account, which, after the victim's approval, are sent to the fraudster (Bulatov, 2015).

A variation of auction fraud on the internet is the so-called "penny auction," where the item is listed at a price of 1–2 dollars, and participants make minimal bids, while a certain amount is deducted from participants with each bid. In the end, victims lose money and do not receive the auctioned item (Queensland Police Service, 2021).

3.4. Traditional Fraud Using Information and Telecommunication Technologies

The next sector of fraudulent actions we want to analyze is traditional fraud using information and telecommunication technologies. The peculiarity of this sector is that such socially dangerous acts can be considered traditional when committing fraudulent actions, but by transferring them into the framework of cyberspace, they acquire greater social danger. Fraud in which a phone or other similar telecommunication gadget serves as the main tool for committing a criminal offense gained active development at the beginning of the 21st century. The emergence of social networks, messengers, and other virtual means of communication only intensified the activity of fraudsters in this sector. Unlike traditional fraud, where the person committing the criminal offense carefully plans to commit one or several socially dangerous acts, telephone fraud in cyberspace

is mostly aimed at mass targeting, where the implementation of the act is replaced by the number of potential victims. Such features as remoteness and the absence of physical contact between the fraudster and the victim only increase the level of social danger. It should be emphasized that we consider the sector of telephone fraud exclusively in the context of those criminal offenses that involve direct communication between the victim and the fraudster, and the implementation of fraudulent schemes directly depends on the social engineering skills of the person committing the criminal offense.

Probably one of the most popular schemes among telephone fraudsters is "phone scamming." Phone scamming is an activity aimed at persuading the victim to transfer funds or obtaining personal, work, banking, or corporate data of the victim that are of interest to the fraudster, for the purpose of use or sale to third parties, conducted through telephone conversations or via the internet, based on social engineering skills.

In the early 2010s, phone scamming was accompanied by primitive deception schemes aimed at vulnerable categories of the population, namely the elderly. The most popular scheme, which fraudsters successfully use to this day, is "your relative is in trouble." Fraudsters, posing as doctors or police officers, call citizens asking them to help a relative solve a problem or avoid responsibility for money. This is one of the most common methods fraudsters use to deceive elderly people. For instance, in early August in Vinnytsia, an 82-year-old pensioner gave 300,000 hryvnias to a stranger. A "doctor" called her and reported that her daughter had been in an accident and money was needed for treatment. The perpetrator was detained; he turned out to be a 34-year-old resident of the Donetsk region, previously convicted for a similar crime (SUSPILNE, 2022).

Another type of "phone scamming" that fraudsters actively use in their activities is calls from bank employees, known as the "bank employee" scheme. The essence of this scheme is that the fraudster, posing as a bank employee or security officer, tries to find out the bank card details, internet banking password, and CVV code, subsequently misappropriating the victim's funds. Such fraudulent actions are carried out in several stages, with a certain time interval between each, and are conducted by an organized group. For example, in the first stage, the fraudster, having certain background information about the cardholder, may ask clarifying questions, information about which the fraudster already has, but this creates certain preconditions and trust from the victim. At this stage, the main task of the fraudsters is to find out how much money the victim has in their card account. In the next stage, the fraudster calls the victim, posing as a bank security representative, and under the pretext of possible danger to their account, persuades them to withdraw money from the main account and transfer it to the bank's reserve account. As a result, the victim loses their funds (National Police of Ukraine, 2021).

The targeted method, unlike the mass one, is aimed at a specific category of people and involves prolonged communication with the victim. An example is the currently popular "victims during the war" scheme, where fraudsters convince the victim that they have lost their home and need money to live, attaching fake photos and videos. Very often, we have situations where fraudsters, pretending to be military personnel, ask for money for fuel, military clothing, or drones.

"Fraud shaming" is a subtype of fraud whose target audience is minors, but often adults who lack legal awareness fall into the fraudsters' trap. The essence of the scheme is that the victim receives a message about committing criminal actions by visiting prohibited web resources of criminal or dubious content or leading an immoral lifestyle. Fraudsters intimidate the victim that such supposedly socially dangerous actions will be reported to law enforcement agencies, media, acquaintances, or relatives unless the person transfers a sum of money determined by the fraudsters. The victim, incorrectly assessing the situation, mainly due to their minor age and the threat of negative consequences in the form of informing their parents or law enforcement agencies about such activities, transfers funds to the fraudsters.

The last subtype of fraud in this sector is scammer calls to the victim by pseudo-representatives of companies like Microsoft, Dell, or McAfee, who report a serious infection of the victim's personal computer with malicious software that could affect the computer's functioning and lead to its complete inoperability, offering to sell software to fix it (Fortinet, 2023).

3.5. Fraud in the Provision of Financial Services

The last sector of fraudulent actions we want to analyze is the financial sector or fraud in the provision of financial services. One of the methods of committing fraud in cyberspace is fraud in the lending sector. There are many financial institutions and banks on the internet that provide microcredit services only with passport data. Funds in this case are credited to the client's card accounts. Currently, such services are very popular; they are used when a person lacks personal funds to pay for a certain product and does not want to buy the product on credit. A fraudster can take loans in someone else's name by providing another person's passport data to the financial credit institution (Liga Zakon, 2021).

Note that this method of fraud is committed without special software or technical means or by interfering with the functioning of means of storing, processing, or transmitting digital information. It can be committed both in cyberspace and by traditional offline methods; the difference will only be in the method of obtaining credit funds (cash or non-cash card transfer) and the avoidance of physical contact with financial institution employees, which significantly increases the latency and social danger of the analyzed method of committing fraud in cyberspace.

The peculiarity of this method of committing fraud in cyberspace lies in the bank card to which the fraudster

receives the credit funds. In most cases, fraudsters create a network of "drop bank cards." A "drop" or "money mule" is a person who agrees to let their bank card become a "transit" for money stolen by fraudsters. The drop transfers illegally obtained funds between different accounts. Such a chain of transfers is needed to confuse the tracks of cybercriminals and complicate the investigation (Cyberpolice, 2017). Very often, "drops" do not even suspect that they have become accomplices in a criminal offense.

3.6. Impact of the War on Changes in Cyber Fraud Models

The military conflict between Ukraine and the Russian Federation has significantly influenced the landscape of cyber fraud, particularly concerning new methods of deception and abuse of trust within cyberspace. With the onset of the war, Ukraine became the target of massive cyberattacks on energy, financial, communication, and governmental structures, and its citizens increasingly fell victim to cybercriminals. These attacks aimed to destabilize the country, lower the morale of the population, and undermine its defensive capabilities.

With the advent of internet usage in Ukraine and the development of various information and telecommunication technologies, fraudsters began exploiting them as opportunities and tools for their criminal activities (Levkivska, 2022). The appeal lies in the inability to see the person directly or have contact with them, which attracts cybercriminals and prompts the development of various criminal schemes to seize property, funds, and valuables from others.

It is essential to emphasize the peculiarities of cyber fraud under martial law conditions, notably:

a) All socially dangerous actions in cyberspace are committed online (cybercriminals use digital platforms to carry out illegal activities, complicating the identification of such individuals);
b) Fraudulent actions are perpetrated during a military conflict, creating additional opportunities for fraudsters due to weakened control and a rapidly growing number of victims;
c) Exploiting the vulnerable state of the population, fraudsters manipulate feelings of empathy and anger;
d) There is misuse of the high demand for vital services, such as evacuation from dangerous territories, rental housing for displaced persons, and payment programs for internally displaced individuals (Herrero et al., 2022).

The conditions of armed aggression by the Russian Federation have significantly heightened the emotional vulnerability of the Ukrainian population. Continuous stress, fear for personal and loved ones' lives, uncertainty about the future, and a general sense of danger weaken citizens' psychological resilience. This state makes them more susceptible to the manipulative techniques used by malefactors to achieve their unlawful objectives.

Cyber fraudsters actively respond to these changes by adapting their fraudulent schemes to new social conditions, leveraging current issues and circumstances related to martial law to enhance the effectiveness of their actions. For instance, cybercriminals create fake charitable foundations to collect funds for victims, offer non-existent evacuation services from dangerous zones, or implement fraudulent schemes involving the sale of scarce essential goods. Thus, malefactors exploit the emotional vulnerability and social needs of citizens, complicating efforts to combat such fraud manifestations.

Focusing on the geography of cyber fraud, under martial law in Ukraine, cyber fraud spans all regions of the country without exception. A significant increase in the number of such offenses is observed, associated with general destabilization, mass population movements, and heightened citizen vulnerability. According to data from the Office of the Attorney General for 2023, 5,842 cases of fraudulent actions in information and telecommunication networks were registered, which is 65% more than in 2022. In 2024, the situation worsened, and as of June 1, 2024, incidents increased by 44% compared to the previous year (Office of the Attorney General, 2024).

It is crucial to highlight that the vast majority of these criminal offenses are committed by men, who constitute approximately 80% of the total number of malefactors. The age range of these individuals varies from 21 to 55 years, with the highest concentration in the 30 to 42 age group. This trend may be linked to the fact that individuals in this age bracket have sufficient life experience, technical skills, and resources to implement complex fraudulent schemes. Although instances of internet fraud committed by minors are rare, they still cause concern and indicate the need to strengthen preventive work among young people (National Police of Ukraine, 2024). Meanwhile, women make up about 20% of those involved in cyber fraud. They predominantly use social networks and online platforms to post fake advertisements for the sale and delivery of goods or rental of housing.

Statistical data indicate that large cities such as Kyiv, Lviv, Odesa, and Dnipro are hotspots of increased internet fraudster activity. This can be explained by the high population density, more developed internet service infrastructure, and a higher level of digital literacy in these regions. Simultaneously, in border and frontline areas, there is a rise in frauds related to evacuation, humanitarian aid, and other urgent needs of the population under martial law conditions (SUSPILNE, 2023).

Analyzing the evolution of cyber fraud actions under martial law, attention should be paid to the main indicators of fraudulent messages (Table 1).

Table 1. *Indicators of Fraudulent Messages*

Manipulation Techniques	Effects and Responses
Manipulation of Urgency	Cybercriminals often create a sense of urgency to compel individuals to act quickly without considering the consequences. Such messages typically appear to come from banks, well-known brands, or even friends and acquaintances. They may inform about issues with bank accounts, promise monetary rewards, or call for donations. Research indicates that a significant number of users fall for such schemes, especially when they concern the security of financial data or personal information (Cyberpolice, 2023a).
Positive Message Manipulation	This manipulation type is based on eliciting positive emotions and promises of benefits. Phrases like "You're in luck! This is the price at the old exchange rate," "Congratulations, great news!", or "You've won an expensive item with free delivery" aim to prompt action. Notably, many internet users are willing to comply if the message contains positive information. A 2023 study by the Ministry of Digital Transformation of Ukraine on the digital literacy of the population shows that a significant portion of respondents click on links or respond to emails promising financial advantages or other benefits (Ministry of Digital Transformation of Ukraine, 2023).
Time-Limited Demands	Cybercriminals may impose specific demands with a limited timeframe for compliance. This creates additional psychological pressure, prompting immediate action without proper situation analysis. For example, a message may require confirming personal data or changing a password within a short period, threatening account blockage otherwise. Such tactics force users to act impulsively, without verifying the information's authenticity.
Manipulation of Fear and Threats	Malefactors might utilize fear and threats, sending messages about potential account blocking, legal consequences, or other negative events if certain actions are not taken. This prompts recipients to act swiftly to avoid imaginary problems. Such messages may appear to come from law enforcement agencies, tax authorities, or other official institutions (Nikkel, 2020).
Exploitation of Social and Topical Issues	Under martial law, fraudsters often exploit current social themes like charity, assistance to the military or victims, to evoke empathy and prompt action. For instance, they may send fake requests for donations towards treatment or army support. Using such themes increases the likelihood that users will respond without proper verification (Cyber Digest, 2024).

These indicators have catalyzed the emergence of new schemes, methods, and techniques of committing cyber fraud. We propose examining some of them.

A. Fraudulent Fundraising for the Armed Forces of Ukraine or for Vehicles. Currently, within the martial law framework, one of the most widespread schemes involves fictitious fundraising to support the Armed Forces of Ukraine. Fraudsters create fake social media pages, websites, or use messengers to disseminate messages calling for army support. In the context of martial law and active hostilities in Ukraine, there is a significant increase in the need for material support for the Armed Forces (Behind the News, 2024). Citizens, businesses, and the diaspora are actively involved in fundraising for the army's needs, particularly for purchasing vehicles, equipment, and ammunition. However, this patriotic impulse becomes a target for manipulation by fraudsters who exploit citizens' noble intentions for personal gain.

The mechanisms of such frauds are quite diverse. Fraudsters create fictitious charitable organizations or funds that exist only on paper or in the digital realm. They develop professionally designed websites, social media pages, and utilize advertising tools to spread information about fundraising efforts. Often, these resources contain moving stories, photographs of military personnel or victims, eliciting an emotional response from potential donors. Malefactors may also use the names of well-known volunteers or organizations, forging their details and contact

information.

Particularly concerning are cases where fraudsters directly approach businesspeople and entrepreneurs. They may leverage personal connections or impersonate officials from military administrations or state institutions. For example, in the Kyiv region, a group of malefactors contacted business owners on behalf of military administration leadership, requesting financial assistance for the Armed Forces. The scheme's organizer was a foreign national serving a sentence in a colony on occupied territory. The funds received were misappropriated, with dozens of entrepreneurs falling victim (SUSPILNE, 2023a). Another example involves unknown individuals in the Kharkiv region who, on behalf of the Kharkiv Regional Military Administration, disseminated false information about collections for the Armed Forces (SUSPILNE, 2023a). Today, on platforms like Telegram or Facebook, nearly every fifth post is aimed at fundraising for unmanned aerial vehicles, and increasingly, such collections turn out to be fraudulent (SUSPILNE, 2023b).

B. Fake Fundraising for the Treatment of Children Affected by Armed Aggression. Amid military aggression and the humanitarian crisis in Ukraine, assisting victims—particularly children injured during hostilities—has become especially urgent. Many citizens and organizations strive to provide support by donating funds for treatment and rehabilitation. Unfortunately, this noble goal is manipulated by fraudsters who create fictitious volunteer and charitable organizations for personal enrichment. Let's examine the mechanism of this scheme. Firstly, fraudsters establish websites, social media pages, or messenger channels that mimic real charitable organizations. They typically use professional design, official language, and symbols to gain potential donors' trust. Secondly, they employ touching stories and photographs, publishing emotionally charged accounts of children affected by hostilities. These stories are almost always accompanied by photographs obtained from open sources or fabricated using information and telecommunication technologies (Harazd, 2022). The next stage involves active promotion through social media advertising. Notably, fraudsters often collaborate with influencers or use bots to disseminate such information. To enhance public trust, they use forged certificates and licenses of the organizations they claim to represent. Fraudsters frequently utilize various crowdfunding methods or target foreign citizens, who have fewer opportunities to verify the information's authenticity (News Life, 2021).

The final stage in successfully implementing this scheme involves using various payment systems to withdraw fraudulent funds. Fraudsters offer convenient methods for transferring money: bank accounts, electronic wallets, cryptocurrency addresses. This complicates tracking financial flows and identifying fund recipients.

C. Fake Receipt of International Assistance. Under martial law and economic instability, many Ukrainians hope for support from international organizations like the UN, the European Union, and other humanitarian institutions. This situation becomes a catalyst for fraudsters to exploit fake resources to extract personal and financial information from users. Generally, the mechanism of this fraudulent activity is straightforward. Fraudsters create convincing phishing resources that mimic real international organizations, select similar domain names, and offer applications for financial aid, compensation, or social payments. Victims are lured to these phishing sites mainly through social media advertising (National Police of Ukraine, 2023).

Users are prompted to fill out forms requiring personal data: full name, address, phone number, identification code, as well as bank card details, including numbers, expiration dates, and CVV codes. After submitting these forms, malefactors gain access to confidential information, which they can use to steal funds or personal data (Ukrainian Helsinki Union for Human Rights, 2022).

D. Fraud Regarding Information on the Whereabouts of Missing or Captured Relatives. The last fraudulent scheme we wish to analyze is not primarily linked to martial law but to generative artificial intelligence systems that facilitate the crime's commission. However, certain elements related to the military conflict serve as auxiliary means to achieve the criminal outcome.

This scheme is implemented by searching for announcements in messengers about missing or captured individuals. Criminals contact the relatives of the missing person, claiming that for a certain fee, they can provide information about their whereabouts. Often, fraudsters state that the missing individual was injured during a combat mission and is currently receiving medical treatment. This type of fraud preys on the emotional vulnerability of people searching for their loved ones. Fraudsters promise assistance but cease communication after receiving payment. Consequently, relatives receive no information about the missing person and suffer financial losses and additional stress (UKRINFORM, 2024).

Due to individuals' misplaced confidence, susceptibility to deception increases. Malefactors use messages that do not arouse suspicion, containing safe, neutral announcement texts requiring a link to be followed. As a result, individuals neglect to verify internet platforms, do not check reviews about products and sellers, and immediately pay for goods without verification, collecting them from postal offices. There are also numerous cases where people do not verify charitable funds or even the truthfulness of information from friends or acquaintances about the help they supposedly need, for which unknown individuals are collecting money. When renting housing, they send funds in advance, relying solely on internet photos of the premises (Moroz et al., 2023).

All this necessitates the introduction of new, often unconventional approaches to organizing and implementing countermeasures against organized criminal manifestations. It is also important to remember that the system of individual preventive measures should be cyclical: starting with actions to eliminate the causes and conditions of

committing socially dangerous acts, continuing with measures to prevent and halt them, and concluding once again with actions to eliminate the causes and conditions of such acts.

4. Legal and Criminological Measures for Preventing and Combating Financial Fraud in Cyberspace

Legal measures are aimed at addressing one of the primary conditions contributing to economic cybercrime—the imperfection of legislation. They include proposals to improve laws concerning criminal liability for economic crimes and offenses in the field of computer information; legislation on information, communications, and personal data. Legal measures are inextricably linked with organizational ones, as they ensure their implementation at the legislative level (Akinbowale et al., 2024). Without proper legal regulation, most organizational measures will be ineffective. It is worth emphasizing that, in fact, no criminal legislation of any state places emphasis on the means of committing a criminal offense, particularly regarding the use of elements of information and telecommunication technologies as factors that aggravate socially dangerous acts.

When analyzing legal measures for preventing and combating cyber fraud, it is worth focusing specifically on international legal initiatives. The absence of clearly defined boundaries in cyberspace creates significant difficulties in bringing perpetrators to criminal responsibility. In our opinion, the only viable solution to the problem of transnational cybercrime is international cooperation.

Currently, more than ever, Ukraine is actively participating in international efforts to combat cybercrimes, particularly economic ones. Over the past fifteen years, Ukraine has concluded a number of agreements on cooperation in the field of combating cybercrime. These agreements envisage joint activities of states in fighting computer crimes, offenses in the sphere of computer information, cybercrimes (including economic ones), and are also aimed at ensuring cybersecurity and protecting cyberspace. However, interstate agreements, in our view, are only the initial stage in the real international fight against cybercrime. At this stage, the main rules and principles of counteraction are formulated, key terms and concepts are defined, and the main directions of the struggle are established. The next step should be the adoption of a Convention under the auspices of the United Nations.

We believe that the Convention should consist of two parts. The first part should provide definitions of cybercrime and cyberspace, as well as a detailed list of types of cybercrimes. The second part should establish a set of measures to counter the transnational nature of cybercrime, define the jurisdiction of states, and lay the foundations for international cooperation in this sphere. It is important that the provisions of this Convention do not violate the sovereignty of states and their legitimate interests. The measures provided in the Convention should be aimed at protecting the rights and freedoms of citizens, the restriction or violation of which, in our opinion, is unacceptable.

Another legal measure to counter this destructive phenomenon involves changing national legislation and adapting it to modern digital realities and key cybersecurity strategies. Here, we believe the main element of a successful concept should be the penalization of certain socially dangerous acts that exhibit signs of fraud but, due to imperfect legislation, are not considered crimes. At the same time, we propose that the means of committing crimes, particularly the use of information and telecommunication technologies, should be introduced as an aggravating circumstance.

In our view, for effective counteraction to economic crimes committed in cyberspace, and cybercrimes in general, countries should primarily adopt their National Cybersecurity Strategies. Such a strategy should define key concepts (cyberspace, cybercrime) and principles of countering cyber threats, as well as outline the main directions of governmental activities in combating cybercrimes.

Based on the analysis of foreign cybersecurity strategies and the National Cybersecurity Strategy of Ukraine, the main directions should include (Decree of the President of Ukraine, 2021):

i. Protection of strategic and state assets (energy, oil and gas complexes, military-industrial complexes, housing and communal services, etc.);
ii. Ensuring the security of citizens, organizations, and the state in both the sphere of computer information and economic relations (property and economic activity);
iii. Improvement of legislation;
iv. Combating anonymity in cyberspace;
v. International cooperation;
vi. Development of specialized law enforcement agencies;
vii. Advancement of information technologies;
viii. Enhancing the digital literacy of the population.

Criminological measures for preventing and combating fraud in cyberspace have been divided into informational-criminological and technical-criminological.

Among informational-criminological measures, we consider the primary one to be the prevention of cybercrime by raising the overall level of cyber hygiene and literacy among citizens. These ideological measures represent a comprehensive set of methods and means aimed at eliminating antisocial attitudes in certain groups and

individuals, as well as forming a negative public attitude towards cybercriminals. They include activities of traditional and internet media, lessons in schools and higher educational institutions, professional development courses, and so forth. However, specific ideological measures will be most effective only for certain audiences (Afzal et al., 2024).

Given the decreasing average age of cybercriminals and their victims, as well as the increasing number of juvenile offenders, the most effective method of ideological influence on them is informing about cybercrimes and the criminal liability for their commission via social networks. The popularity of various social networks among minors is a necessary condition for effective prevention of cybercrime. Considering that over 75% of children have a profile on social networks, with almost a third having more than one profile in different networks and visiting them almost daily, such prevention will be maximally effective. Moreover, since the use of computers and the Internet begins at an early age (5–6 years), the culture of information security needs to be instilled from this age. It is necessary to develop in cyberspace users a stable habit of checking their computers for viruses, installing protective programs, and updating them in a timely manner. It is believed that such a useful habit should be inculcated from childhood, like brushing teeth or washing hands (Whitty, 2020).

We must highlight Ukraine's experience in this matter, particularly regarding mass warnings and reminders to citizens about new fraudulent schemes via SMS messages sent by cyber police authorities. Every week, the press center of the Cyber Police Department of the National Police of Ukraine sends information about current cybercrime schemes via mobile operators or messengers, emphasizing how not to become their victim. This activity is extremely important for elderly people, as they often rely on SMS to familiarize themselves with cybercrime trends and avoid becoming victims in the future (Cyberpolice, 2023b). Arguably, one of Ukraine's main achievements in combating cybercrime during the war was the creation of the "BRAMA" project with the support of the Cyber Police Department of the National Police of Ukraine. The "BRAMA" bot is an effective tool in preventing and combating cyber fraud thanks to several key mechanisms: 1) detection and blocking of malicious resources; 2) ability to report suspicious websites, social profiles, and other online resources that may be associated with fraud or disinformation; 3) analysis of received information by cyber police specialists to determine its authenticity and potential threat; 4) blocking of malicious resources upon confirmation, preventing access to them and further spread of fraud (Kharkiv Regional Prosecutor's Office, 2024).

It is also worth highlighting that the bot performs an important informational function by informing citizens about current threats in cyberspace. It provides up-to-date information about new fraudulent schemes, phishing attacks, and other cyber threats. Additionally, the bot offers recommendations on cyber hygiene, providing advice on safe internet use, protection of personal data, and recognition of fraudulent resources. This contributes to raising public awareness and fostering a culture of safe behavior in the digital environment.

Separately, the involvement of active users in combating cyber fraud should be noted, as it motivates them to report suspicious resources and activities. This creates a platform for exchanging experiences and information between users, experts, and law enforcement agencies, thereby increasing the effectiveness of countering cyber threats. Forming an active community contributes to faster and more effective responses to new challenges in the field of cybersecurity. Also, the bot facilitates educational activities by distributing learning materials, articles, and videos aimed at increasing the digital literacy of the population. It informs citizens about webinars, training sessions, and other events where they can learn more about cybersecurity and ways to protect themselves from fraud. This is especially important in the context of the constant growth of cyber threats and the rapid development of technologies used by malefactors. As technical-criminological measures, we propose special mechanisms and methods of information control aimed at countering the anonymity of economic cybercrimes and technically improving cyberspace itself.

5. Countering Anonymity

In our opinion, countering the anonymity of cyberspace users and information networks is one of the key principles in combating both economic cybercrime and cybercrime in general. Due to the features of modern technologies, it is impossible to accurately determine who was at the computer at the moment of committing a cybercrime, since users interact not directly but through their accounts. Anyone can claim that during the commission of the crime, someone else was at the computer who simply used their account for illegal actions. Even when identifying the IP address or MAC address of the device, this problem remains relevant, significantly complicating the work of law enforcement agencies and leading to a high level of latent crime (Levi et al., 2017).

The most effective solution is the personalization of cyberspace users. Any person who uses the Internet or other information and telecommunication networks should leave their unique trace. Such a trace can be a passport number, electronic signature, facial photograph, or fingerprint. Nevertheless, the best practice is in combating anonymity is the development and implementation of biometric technologies, such as facial recognition and fingerprint scanners. Almost all new computers, laptops, smartphones, and tablets have built-in cameras capable of recognizing the user's face using special software. This software can be integrated, for example, into mobile banking applications. During each financial transaction, the application will require the user to bring the camera to their face, and if the biometric data matches, it will allow the operation. In the future, when such technology becomes automated, it can be implemented in social networks as well. Then, when a fraudster or extortionist

communicates with a victim on the Internet, their biometric data will be recorded.

With large-scale implementation of such technology, cyberspace users will leave indisputable traces of their activities—their facial images. The advantage of this technology is that there are no intermediaries between the cyberspace user and their account in the form of logins, passwords, internet passports, or flash devices. The computer automatically identifies the user based directly on their biometric data. Another benefit of facial recognition technology is that it can be widely implemented today. As per our opinion, personalization of cyberspace users is the only solution to the problem of anonymity, and its implementation is already a matter of technology.

6. Conclusion

The increased vulnerability to deception in cyberspace is largely due to individuals' misplaced confidence in their ability to recognize fraudulent activities. This false confidence makes people more susceptible to manipulation by fraudsters. Today, scammers use messages that, at first glance, do not arouse suspicion, containing neutral advertisement text and prompting users to click on certain links. As a result, users neglect to verify online platforms, do not research reviews of products and sellers, and, without additional checks, immediately pay for goods, collecting them from postal outlets. This approach leads to citizens becoming victims of fraud, losing their financial resources without the possibility of recovery. A significant number of cases also involve situations where individuals do not verify the legitimacy of charitable foundations or the truthfulness of information received from friends or acquaintances about necessary assistance for which unknown persons are collecting money. This is particularly relevant in conditions of military conflict, when the number of charitable initiatives increases, and fraudsters exploit the emotional state of the population. Studies show that about 40% of citizens are willing to make donations without verifying information if it concerns help for war victims (Report Zagoriy Foundation, 2022).

All these problems require the introduction of new, often unconventional approaches to organizing and implementing countermeasures against organized criminal activities. In particular, it is important to develop comprehensive strategies that combine legal, social, and technological measures. It is also crucial to remember that the system of individual preventive measures should be cyclical: starting with actions to eliminate the causes and conditions of committing socially dangerous acts, continuing with measures to prevent and stop them, and concluding again with actions to eliminate the causes and conditions of such acts. This approach will ensure systematicness and effectiveness in combating cybercrime.

The importance of educational work is confirmed by statistical data. According to a survey conducted by the Institute of Cybersecurity, the population's awareness of internet fraud methods can reduce the risk of becoming a victim by 35%. Thus, informational support is one of the most effective tools for preventing cybercrime. Timely updated information about new types of online fraud, methods of their commission and concealment, behavioral characteristics of fraudsters, and criminogenic trap situations they create for criminal encroachments is critically important. The development and dissemination of explanatory instructions on recognizing scam schemes on the internet, and advice on counteracting these crimes, can also significantly reduce the level of such criminal offenses. According to research conducted by the European Cybercrime Centre, comprehensive preventive measures can decrease cybercrime levels by 30% (EU4Digital, 2023). In the context of martial law, special attention should be paid to protecting vulnerable categories of the population, who may be more susceptible to fraud due to emotional state or lack of access to reliable information. Cooperation between state bodies, public organizations, and the private sector is necessary to create an effective system for countering cybercrime.

Acknowledgement

This study is funded by the Ministry of Education and Science of Ukraine and contains the results of the projects No. 0123U101945 “National security of Ukraine through prevention of financial fraud and money laundering: war and post-war challenges”

References

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

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

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

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

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/

Breen, C. F. (2022). *A large-scale measurement of cybercrime against individuals*. Retrieved from

http://surl.li/iavyy

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

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

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

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/

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/

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/

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

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/

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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).

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

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

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

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

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

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

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

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

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

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

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

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/

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/

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/

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

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