DOI: 10.55643/ser.3.53.2024.574

CLASSIFYING CYBERCRIME NETWORKS: ORGANIZED AND TRANSNATIONAL SCHEMES IN THE DIGITAL ERA

Inna Tiutiunyk
D.Sc. in Economics, Associate Professor of the Department of the Financial Technologies and Entrepreneurship, Sumy State University, Sumy, Ukraine;
e-mail: i.tiutiunyk@biem.sumdu.edu.ua
ORCID: 0000-0001-5883-2940
(Corresponding author)

Dmytro Toptunenko
Department of Financial Technologies and Entrepreneurship, Sumy State University, Sumy, Ukraine;
ORCID: 0000-0002-5532-6441

Anna Flaumer
Lecturer, Kolping Academy, Würzburg, Germany;
ORCID: 0000-0003-0596-2199

ABSTRACT

The purpose of this study is to analyze and classify the main schemes of organized and transnational cybercriminal activity, as well as to identify the methods and technologies used by cybercriminals to carry out criminal activities in the digital space. The article explores current trends in cybercrime, such as the rise in financial fraud, ransomware attacks, phishing, and DDoS attacks. The study shows that the use of the latest technologies, particularly cryptocurrencies and the Internet of Things (IoT), significantly complicates the detection and prosecution of cyber criminals, necessitating the constant improvement of legal and technical tools to combat cybercrime. Key findings indicate that the transnational nature of cybercrime often makes it difficult to prosecute criminals across jurisdictions, requiring greater international coordination. It was also found that cybercriminals are using increasingly sophisticated methods to conceal their activities, incorporating modern technological solutions into criminal schemes. This underscores the need for continuous monitoring of new threats and the updating of protection methods for both organizations and individual users. The main conclusions of the study emphasize the importance of global cooperation in the fight against cybercrime, the need to enhance technological protection, and the development of legal mechanisms to counter modern cyber threats.

Keywords: organized and transnational cybercrime, financial fraud, ransomware attacks, phishing, DDoS attacks

JEL Classification: 38, F52, O17

INTRODUCTION

One of the most urgent and important problems of our time is the issue of combating cybercrime. The growing dependence on digital technologies, which cover almost all spheres of social life from the economy to education and healthcare makes cyberspace particularly vulnerable to attacks. According to a report by Cybersecurity Ventures (2020), global losses from cybercrime could reach USD 10.5 trillion per year by 2025. These figures reflect a rapid increase in cybercrime compared to USD 3 trillion in 2015. According to Statista (2024), the number of data breaches worldwide continues to grow, reaching more than 1.1 billion cases in 2023. This significantly exceeds previous years' figures and highlights the increasing activity of cybercriminals.

Improvements in the skills and sophistication of cybercriminals, who use complex and dynamic methods such as phishing, viruses, malware, and social engineering, lead to a growing scale of cybercriminal activity and emphasize the urgency of effective measures to combat it. For example, according to Verizon's Data Breach Investigations Report (2024), about 36% of all data breaches in 2023 were related to phishing and other social engineering methods.

These trends highlight the need for continuous improvement in security measures and increased awareness of cyber threats to reduce the risks associated with cybercrime. The global nature of the Internet further complicates the processes of combating criminal activity in cyberspace and bringing to justice cyber criminals operating from different parts of the world. This requires international cooperation, information sharing, and coordination of legal norms between states to ensure the security and protection of user

Received: 09/09/2024
Accepted: 26/09/2024
Published: 30/09/2024

data. An effective fight against cybercrime includes both technological solutions such as improved data protection and encryption systems and legal and educational measures aimed at increasing public awareness of cyber threats.

LITERATURE REVIEW

Each year, the issue of researching modern approaches to the classification of cybercriminal activity, analyzing organized criminal groups in the digital space, and addressing the challenges associated with transnational cybercrime is gaining increasing popularity. A significant number of scholars focus on studying the methods and schemes of cybercriminals, as technological progress creates new opportunities for committing illegal acts in cyberspace. Such research is centred on developing effective methodologies to combat cybercrime and identifying connections between traditional organized crime and its new forms in the digital world. Particular attention is given to the transnational aspects of this problem, as the activities of cybercriminal groups often transcend national borders, requiring global coordination of efforts to ensure cybersecurity.

In a broad sense, cybercrime can be understood as criminal activity associated with information technologies, network devices, or the network itself. Wall (2007) defines organized cybercrime as crimes systematically committed by criminal organizations using digital technologies as either the main tool or the target. In his research, the author identifies three types of cybercrime: crimes where the computer is the target (e.g., hacking), crimes where the computer is the tool (e.g., fraud), and crimes where the computer is incidental (e.g., storing illegal images).

The transnational nature of cybercrime significantly complicates the definition of the term, the study of its features, and the development of preventive tools. Broadhurst (2006) noted that cybercrime often spans multiple jurisdictions, thereby complicating the legal definition of such activities and the efforts of law enforcement agencies to combat them. Consequently, the fight against organized and transnational cybercriminal activity requires close cooperation between regulatory bodies in different countries, the development of unified legal standards, information exchange, and the creation of international platforms for action coordination. Joint efforts by governments, private companies, and international organizations are essential for ensuring effective counteraction to these threats, especially considering the dynamism and scale of modern cybercrime. Choo (2011) emphasizes the need for international cooperation in identifying and combating cybercrime, given its cross-border nature.

Another crucial component in combating organized criminal activity in cyberspace is identifying all possible schemes for its implementation and studying the mechanisms used by criminals to organize their actions. This includes analyzing methods of communication, the use of anonymous platforms, cryptocurrencies for money laundering, phishing schemes, and various forms of cyber fraud. An important aspect is also identifying key actors and structures coordinating organized groups, as well as tracking their connections with other criminal networks. A deep understanding of these schemes allows law enforcement agencies not only to investigate crimes more effectively but also to anticipate potential threats and develop proactive measures to prevent criminal activity in cyberspace.

In the scientific literature, various types of cybercriminal groups are distinguished: organized, transnational, autonomous, and specialized.

Organized cybercriminal groups have a clearly structured hierarchy and long-standing connections between members, allowing them to coordinate complex operations, such as financial fraud, and cyberattacks on large corporations, or government institutions. Hutchings (2018) describes these groups as having a hierarchical structure with clear roles, such as planners, coders, money mules, and enforcers. They often engage in activities like ransomware attacks, financial fraud, and identity theft.

Transnational groups operate beyond national borders and often involve participants from different countries, using differences in legislation to avoid accountability. They frequently engage in international crimes, such as money laundering, human trafficking, and drug trafficking using digital technologies. According to Leukfeldt et al. (2017), these networks exploit global discrepancies in cybercrime laws and law enforcement, using jurisdictions with weaker cybercrime laws as safe havens. They are involved in various activities, from hacking and data leaks to more complex crimes, such as industrial espionage and state-sponsored attacks.

Autonomous groups operate independently, without formal structure or leadership, but can quickly organize to carry out specific tasks or attacks. These groups often use social networks and forums to coordinate their actions. For instance, Hutchings & Clayton (2016) analyzed the activities of autonomous groups and specialized cybercriminals providing DDoS attack services over the internet.

DOI: 10.55643/ser.3.53.2024.574

Specialized groups focus on specific types of cybercrimes, such as writing malicious software, data theft, or cryptojacking (illegal cryptocurrency mining), often selling their services on the black market to other criminals or organizations. In Choo's (2011) research, specialized cybercriminal groups involved in creating malware and offering cybercrime services on demand were analyzed.

Lusthaus (2018) introduced the concept of hybrid groups, which operate within both organized crime and cybercrime. These groups may engage in both traditional crimes (e.g., drug trafficking) and cybercrimes (e.g., phishing or ransomware), using profits from one to fund the other.

The results of the literature review confirm the existence of a wide range of types of criminal activity, the list of which is constantly expanding under the influence of rapid digital technology development. Traditional forms of crime, such as fraud, money laundering, and data theft, are taking on new forms in the online space, complicating their detection and investigation. In this context, the study of cybercrime schemes becomes increasingly relevant, considering the current realities of technological development, including the emergence of new tools and platforms for committing crimes. Such research provides a better understanding of the mechanisms used by criminals and enables the adaptation of legal and technical measures to combat cybercrime.

AIMS AND OBJECTIVES

The purpose of this study is to analyze and classify the schemes of organized and transnational cybercriminal activity and to identify the main methods and tools used by criminals in the digital space. The research aims to identify key factors contributing to the spread of cybercrime, as well as to study the structures and patterns of interaction between members of cybercriminal groups. Additionally, special attention is paid to the transnational nature of cybercrime, which highlights the difficulties associated with coordinating international efforts to combat these crimes and provides the basis for developing recommendations to improve legal and technological measures for effective counteraction.

METHODS

The study of organized and transnational cybercriminal activity schemes will be conducted using general scientific research methods, such as analysis, synthesis, induction, and deduction. The analysis will allow for a detailed examination of existing cybercriminal activity schemes by breaking them down into separate components for a deeper understanding. Synthesis will be employed to combine the gathered data and create a generalized picture of criminal activity in the digital space. Induction will be used to formulate general conclusions based on specific facts and cases of cybercrime, while deduction will help test hypotheses and identify patterns in the actions of criminal groups. Additionally, a comparative method will be applied to assess various types of criminal activity, and a systematic approach will be used to account for the relationships between the elements of cybercriminal schemes, providing a better understanding of the functioning mechanisms of these groups.

RESULTS

The active development of digital technologies is accompanied by the continuous expansion of cybercriminal activity schemes. New technological advancements not only create vast opportunities for economic and societal development but also give rise to new mechanisms that are actively exploited by cybercriminals. Criminal groups are constantly adapting to changes, and refining their methods and tools, including through the use of malware, phishing, DDoS attacks, money laundering via cryptocurrencies, and other modern technologies. In this regard, identifying and categorizing cybercriminal activity schemes is essential for implementing effective cybersecurity measures, which are critical for ensuring the protection of states, businesses, and citizens in the digital era.

One of the most common cybercriminal schemes is financial fraud. This criminal activity aims to illegally obtain financial benefits through manipulation, deception, and abuse in the digital space. Financial fraud encompasses a wide range of activities, including phishing, identity theft, credit card fraud, money laundering through cryptocurrencies, and fake investment schemes. According to Norton (2023), financial fraud caused losses of more than USD 5.8 billion globally in 2023. This figure includes all types of fraud, from phishing to identity theft.

According to a report by the FBI's Internet Crime Complaint Center [**Помилка! Джерело посилання не знайдено.**], the number of incidents of financial fraud over the Internet in 2022 increased by 20% compared to the previous year, with

losses reaching USD 3.5 billion in the United States alone. Additionally, Statista reports that total losses from credit card fraud in the U.S. were approximately USD 12.6 billion in 2021. The World Bank estimates that between 2% and 5% of global GDP, equivalent to roughly USD 800 billion to USD 2 trillion, is laundered annually.

Modern cybercriminals actively utilize the internet, anonymous payment systems, social networks, and various technological tools to carry out fraudulent operations. Particularly concerning are schemes that span multiple countries, making it more difficult to identify the criminals and bring them to justice. The main methods of financial fraud are:

1. Credit card fraud, which involves the theft or illegal use of credit card data for unauthorized purchases.
2. Phishing, which refers to attacks aimed at obtaining confidential information, such as bank details or account logins.
3. Money laundering, a process through which criminals attempt to legalize illegally obtained income by using anonymous payment systems or cryptocurrencies.
4. Stock market fraud, which includes the manipulation of shares and other financial instruments to obtain illegal profits.
5. Internet fraud, which involves the use of online tools to deceive victims, for example through fake investment schemes, phishing websites, or fraudulent online stores.

The prevalence of financial fraud is due to the ease of access to digital technologies and the low awareness of many users about methods of protecting their financial data, making them easy targets for cybercriminals.

Money laundering is a key element in the financial schemes of organized criminal groups, terrorist organizations, and corrupt entities. It is the process of concealing the source of illegally obtained funds, allowing criminals to use this money in the legal economy without revealing its origin.

The main purpose of money laundering is to make illegally obtained funds appear legitimate. This can be achieved through complex financial transactions involving the use of offshore accounts, shell companies, and cryptocurrencies, which ensure anonymity and minimize the risk of detection. Modern technologies, particularly the Internet and digital platforms, have greatly facilitated this process, allowing transactions to be conducted with minimal involvement from regulatory authorities.

Money laundering is not only an economic crime but also a means of financing other criminal activities, such as drug trafficking, arms smuggling, human trafficking, and terrorism. This has serious consequences for national economies, undermining financial stability, promoting corruption, and damaging the reputation of banking and financial institutions.

The process consists of three stages: placement (criminal proceeds are introduced into the financial system through small deposits or asset purchases); layering (multiple transfers of funds through different accounts, businesses, or investments to obscure their origin); and integration (after several transactions, criminal funds appear "clean" and can be used for legitimate purchases, investments, or operations).

According to the UN, 2% to 5% of global GDP is laundered annually, amounting to USD 800 billion to USD 2 trillion. Chainalysis (2022) estimates that USD 8.6 billion was laundered through cryptocurrencies in 2022, highlighting the growing role of cryptocurrencies in criminal operations. According to FATF, banks remain the main point for the placement and layering of criminal funds, particularly through offshore accounts and complex international company structures.

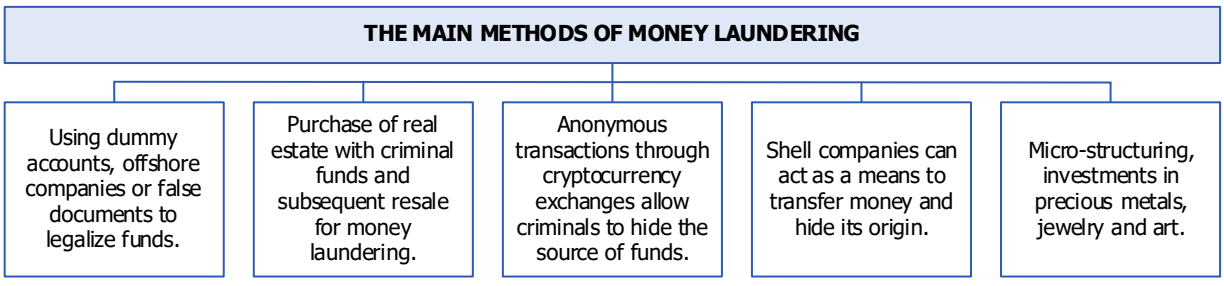

Figure 1. Main methods of money laundering.

Money laundering has a negative impact on the economy, as it creates an unequal market environment, promotes corruption, and damages the reputation of financial institutions. It also facilitates the financing of other crimes, such as terrorism, drug trafficking, and arms smuggling.

With the active use of computer technology across all sectors of the economy, the use of malicious software (malware) in criminal schemes has been rapidly evolving. Malware refers to any program or file designed to harm computers, networks,

DOI: 10.55643/ser.3.53.2024.574

or users. According to AV-TEST, more than 560,000 new malware instances were detected daily in 2023. The number of attacks is continuously rising, particularly due to the spread of ransomware and spyware.

Malware is created to disrupt systems, steal sensitive data, track user activity, or cause other harm. This type of software can spread through email, infected websites, social networks, file downloads, and even through legitimate applications. The most common types of malware include:

- viruses, which are programs that attach to other programs or files and execute together with them. Viruses can damage or delete files, slow down your system, or cause a program to crash;
- trojans that masquerade as legitimate programs but perform malicious actions, such as stealing passwords or installing remote access backdoors;
- worms that propagate through networks independently, without the need for user interaction, and can cause network failures by multiplying and overloading resources;
- ransomware blocking access to files or the system, demanding a ransom for their restoration;
- spyware, which are programs that secretly collect information about the user or his actions on the computer, often for commercial or criminal purposes;
- adware (advertising software) that displays unwanted advertisements on the user's computer or redirects to advertising sites, often changing browser settings.

The use of malicious software is characterized by its difficulty of detection (many types of malware hide within systems, making detection challenging without specialized antivirus or anti-spyware software), rapid spread (some types of malware can spread independently through networks, allowing them to infect large systems in a short period), the anonymity of cybercriminals (malicious software enables criminals to remain anonymous, especially when using ransomware or remote access Trojans), the scale of attacks (malware can target both individual users and large organizations or government institutions), and destructive consequences (ranging from the loss of personal data and financial losses to damage to critical infrastructure).

It is quite common for attackers to impersonate trusted organizations or individuals, using emails, messages, or fake websites to trick users into voluntarily providing their data. According to Statista, the number of phishing attacks worldwide in 2023 exceeded 4.5 million incidents per month, highlighting the increasing activity of cybercriminals. In the U.S. alone, total losses from phishing attacks in 2022 surpassed USD 2 billion, with financial institutions and technology companies being the most affected.

Phishing, a type of cybercriminal activity aimed at obtaining confidential user information such as logins, passwords, credit card numbers, or other personal data through deception, can be carried out in various forms, including:

- email phishing, where an attacker sends an email that looks like a message from a known organization (for example, a bank, support service, online store), with the aim of forcing the user to go to a fake site and enter their data;
- smishing, in which attackers send fake text messages, usually containing links to malicious websites or calls to action, for example, to confirm a bank transaction;
- vishing, which is phishing through phone calls, when criminals try to get confidential information through phone conversations, posing as representatives of banks, technical support or government services;
- targeted phishing aimed at a specific person or organization. This is a more sophisticated type of attack, where criminals collect information about the victim (for example, through social networks) and use it to create more believable messages;
- phishing sites that imitate real sites of banks, shops or other services in order to force users to enter their data.

Phishing is one of the most widespread and dangerous forms of cybercrime, constantly evolving. Its success is largely based on deception and user trust, making it effective even in the digital age, where one might assume that most users are aware of threats. Effective protection against phishing requires a combination of technological tools, such as email filters, and educating users to recognize the signs of potentially dangerous attacks.

Phishing attacks often result in significant financial losses for both individual users and companies, which may lose money or suffer data theft. Users may have their personal data, including credit card numbers, passwords, or other sensitive information, stolen and used for further criminal activity. When a phishing attack targets a company, it can lead to breaches of corporate systems, the loss of confidential data, and damage to the company's reputation.

A Distributed Denial of Service (DDoS) attack is a type of cyberattack in which attackers attempt to disable or slow down an internet resource, website, or network service by overwhelming it with requests from multiple devices or systems simultaneously. The goal of a DDoS attack is to render a resource unavailable to legitimate users by overloading the servers or network it relies on.

DDoS attacks are typically carried out using botnets a network of infected devices (computers, servers, routers, IoT devices) controlled by cybercriminals. These devices, often without their owners' knowledge, are used to send massive amounts of requests to the target server or network. The proliferation of IoT devices has made DDoS attacks even more powerful, as such devices often have weak security protections and are easily compromised.

According to data from Cloudflare, more than 15 million DDoS attacks occurred in 2022, indicating a significant threat to internet infrastructure. The largest DDoS attacks have been recorded with peak traffic exceeding 3 Tbps, demonstrating the ability of these attacks to scale to massive volumes, especially through the use of botnets composed of IoT devices. According to Kaspersky, the financial sector, government institutions, and e-commerce companies are the most vulnerable to DDoS attacks. In 2023, more than 60% of attacks were directed at financial services. Cisco reports that global losses from DDoS attacks amount to USD 20 billion annually, as downtime and service disruptions can have a severe impact on businesses. The most common types of DDoS attacks include:

- volumetric attacks. This is the most common type of DDoS attack, in which a large amount of traffic is used to overload the network. An example is a UDP flood attack, where attackers send a large stream of packets that do not require a response, draining server resources.
- protocol attacks aimed at exhausting network protocol resources. An example is SYN flood attacks, in which connection requests are sent without completing the connection establishment process.
- application layer attacks aimed at exhausting server resources by sending a large number of requests to a specific web service or application. An example is HTTP GET/POST attacks, where the server is forced to process many requests, which reduces its performance.

DDoS attacks remain a serious threat to businesses and organizations worldwide. Their large scale and low cost to cybercriminals make these attacks particularly attractive to attackers. An effective strategy to protect against DDoS attacks requires a combination of technological solutions, such as traffic filtering and load balancing, along with increased organizational awareness and preparedness to respond to these threats. Downtime caused by DDoS attacks can result in significant revenue loss, especially for businesses that rely on online sales or internet-based customer services. Companies targeted by DDoS attacks may also lose customer trust if they are unable to quickly restore their services. Moreover, DDoS attacks can disrupt not only individual websites or servers but entire networks or even critical infrastructure, with serious consequences for society.

The results of the analysis indicate a wide range of cybercriminal activity schemes (a comparative analysis is provided in Table 1), each with its own unique implementation features, which determine the specific methods of their identification and prevention. Each type of criminal scheme requires a tailored approach to detection and prevention, considering differences in the technologies used, attack methods, and the level of resources involved. Therefore, it is crucial to develop comprehensive and flexible strategies to combat cybercrime, enabling swift responses to new threats in the digital environment.

DISCUSSION

The results show that modern cybercrimes are complex and dynamic in nature, constantly evolving alongside the development of digital technologies. A key aspect is that cybercrime is often transnational, making detection and investigation challenging and requiring cooperation between countries and international organizations.

The wide range of cybercrime schemes including financial fraud, money laundering, malware, phishing, and DDoS attacks necessitates a comprehensive approach to detection, analysis, and countermeasures. Cybercriminals continuously expand and refine their methods, leveraging the latest technologies to bypass traditional defences. This calls for constant updates to technological solutions, the development of new protection and monitoring methods, as well as close collaboration between government agencies, the private sector, and international organizations.

One of the main challenges is the adaptability of cybercriminal groups to new technological opportunities, such as artificial intelligence, the Internet of Things (IoT), and cryptocurrencies. These technologies not only provide new means for criminal activities but also complicate the process of tracking and prosecuting offenders. The use of botnets in DDoS attacks,

DOI: 10.55643/ser.3.53.2024.574

the anonymity of cryptocurrencies in money laundering, and new social engineering techniques in phishing schemes make these threats increasingly difficult to combat.

Another important aspect is that financial fraud remains one of the most prevalent types of cybercrime, causing significant economic losses for both individuals and large organizations. The use of cryptocurrencies in money laundering illustrates how cyber criminals increasingly rely on technological means to conceal their activities.

Despite the ongoing development of protective technologies, cybercrime remains highly resistant to new countermeasures. For example, while spam filters and antivirus programs continue to improve, attackers find new ways to circumvent these defences through social engineering or more sophisticated malware.

The study's results also underscore the importance of international cooperation in effectively combating cybercrime. Since many schemes operate across multiple jurisdictions, coordination between states and organizations such as Interpol and Europol become a critical factor in addressing these threats.

Table 1. Comparative analysis of schemes of cybercriminal activity.

Criterion	Financial fraud	Money laundering	Malicious software	Phishing	DDoS attacks
Basic methods	Use of fake sites, theft of bank data	Anonymous payment systems, cryptocurrencies	Use of Trojans, viruses to damage systems	Sending fake emails, social engineering	Overloading the system with crash requests
Goals	Theft of money, illegal financial transactions	Laundering of illegal income	System compromise, data theft	Receiving confidential information	Violation of access to web resources, blackmail
Technologies involved	Harmful websites, phishing programs	Cryptocurrency transactions, anonymous wallets	Trojan programs, viruses	Fake e-mails, fake web pages	Network botnets, special attack tools
Transnational character	Often covers several countries	International transactions and transfers	Can spread over global networks	It is used internationally	Attacks are often carried out from different countries
Motives of criminals	Financial benefit	Financial benefit, avoidance of punishment	Financial gain, personal revenge	Receiving confidential data	Violation of services, blackmail
Scale of operations	Global operations	International operations	International operations	Global campaigns	Global attacks
Target objects	Financial institutions, private individuals	State institutions, financial structures	Large companies, state institutions	Private individuals, corporate systems	Business, government organizations
Frequency and duration of attacks	Permanent operations	Long operations	Permanent attacks	Single Attacks or Campaigns	Short-term attacks
Countermeasures	Technological protection, monitoring	International cooperation, legislation	Antivirus programs, system isolation	Staff training, anti-phishing programs	Traffic filtering, firewalls
Level of technical complexity	Average	High	High	Low or medium	Average

However, one of the key challenges in the fight against cybercrime is the lack of uniform protection standards and regulations across different countries. Some countries have strong cybersecurity laws, while others have limited legislation or technological resources to combat cybercrime. This creates opportunities for criminals to exploit countries with less developed legal frameworks to conduct their operations.

In terms of practical solutions, a combination of technological protections, legal regulations, and educational programs to raise user awareness is essential. Innovative approaches, such as using artificial intelligence to analyze cyber threats, have the potential to significantly enhance the ability to detect and prevent attacks.

Thus, effectively combating cybercrime requires the continuous improvement of technological, legal, and organizational measures. Only an integrated approach combining international cooperation, technological modernization, and increased awareness among users can provide adequate protection against growing threats in cyberspace.

The obtained results provide valuable insights into the expanding scope of cybercriminal activity and the evolution of methods used by cybercriminals. Our analysis shows that financial fraud, phishing, ransomware, and DDoS attacks are among the most common cybercrime schemes. These findings are consistent with previous research by Broadhurst (2006) and Hutchings & Clayton (2016), which also highlight the increasing sophistication and frequency of these attacks. Notably,

our results emphasize the growing role of ransomware and DDoS attacks, which have seen significant growth in recent years, further supporting reports from SonicWall (2022) and Cloudflare (2023).

However, our study has certain limitations. First, cybercrime data is often fragmented due to the nature of the crimes and the lack of comprehensive reporting, making it difficult to capture the full extent of certain attacks. Second, the rapid evolution of cybercrime tactics presents a challenge in ensuring the timeliness of the data. Third, our study mainly focuses on trends observed in specific regions, limiting the generalizability of the findings to other parts of the world with different regulatory and technological environments.

Despite these limitations, our study makes a significant contribution to understanding current trends in cybercrime. Future research should aim to address these limitations by expanding data collection efforts and focusing on emerging technologies that may be exploited in future cybercriminal activities. In conclusion, the findings highlight the growing complexity and scale of cybercrime and the urgent need for enhanced cybersecurity measures, global cooperation, and ongoing research into new protective technologies. These efforts are critical to mitigating the risks posed by cybercriminals and protecting both businesses and individuals in an increasingly digital world.

CONCLUSIONS

The research conducted demonstrated that cybercriminal activity is one of the most dynamic threats of modern times, constantly adapting to new technological conditions. Criminals are increasingly using sophisticated methods such as malware, phishing, DDoS attacks, and money laundering through cryptocurrencies, making them difficult to detect and deter. The transnational nature of cybercrime indicates the need to develop unified international standards and common platforms for information exchange between countries and organizations. Without proper international coordination, the fight against cybercrime remains fragmented and less effective.

In addition, an effective fight against cybercrime requires not only technical solutions but also coordinated actions at both national and international levels. It is also important to implement measures to increase cyber literacy among users, as social engineering remains one of the most frequently used tools by cybercriminals to gain access to information.

Equally important is the role of innovation in the field of cybersecurity. The use of artificial intelligence, automated monitoring systems, and machine learning can significantly improve the ability to identify new threats at an early stage. Such technologies can strengthen existing security systems and prevent more sophisticated attacks.

Overall, the further development of mechanisms for ensuring cybersecurity requires both technological progress and a broad educational campaign among users, as well as cooperation at the global level. This will help create a safer digital environment and reduce the negative impact of cybercrime on the economy and society.

ADDITIONAL INFORMATION

AUTHOR CONTRIBUTIONS

All authors have contributed equally.

FUNDING

This research was funded by the projects "Modeling the mechanisms of combating organized and transnational cybercrime in war and post-war periods" (0124U000550), funding – Ministry of Education and Science of Ukraine.

CONFLICT OF INTEREST

The Authors declare that there is no conflict of interest.

REFERENCES

1. Broadhurst, R. (2006). Developments in the global law enforcement of cyber-crime. *Policing: An International Journal*, *29*(3), 408-433. https://doi.org/10.1108/13639510610684674
2. Chainalysis (2022). The 2022 Crypto Crime Report. https://go.chainalysis.com/rs/503-FAP-074/images/Crypto-Crime-Report-2022.pdf

DOI: 10.55643/ser.3.53.2024.574

3. Choo, K.K.R. (2011). The cyber threat landscape: Challenges and future research directions. *Computers & Security*, *30*(8), 719-731. https://doi.org/10.1016/j.cose.2011.08.004
4. Cloudflare (2023). DDoS Reports. https://blog.cloudflare.com/tag/ddos-reports/
5. Cybersecurity Ventures (2020). Cybercrime To Cost The World $10.5 Trillion Annually By 2025.https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/#:~:text=Cybersecurity%20Ventures%20expects%20global%20cybercrime,%243%20trillion%20USD%20in%202015
6. Federal bureau of investigation (2024). Internet Crime Complaint Center (IC3). https://www.ic3.gov/
7. Hutchings, A. (2018). Crime From the Keyboard: Organised Cybercrime, Co-Offending, Initiation and Knowledge Transmission. *Criminology & Criminal Justice, 18*(4), 488-504. http://dx.doi.org/10.1007/s10611-014-9520-z
8. Hutchings, A., & Clayton, R. (2016). Exploring the Provision of Online Booter Services. *Deviant Behavior*, *37*, 1-16. https://doi.org/10.1080/01639625.2016.1169829
9. Leukfeldt, E., Poot, C., Verhoeven, M., Kleemans, E.R., & Lavorgna, A. (2017). Cybercriminal networks. In book: Research Agenda the Human Factor in Cybercrime and Cybersecurity (pp.33-42). Publisher: Eleven. Editors: R. Leukfeldt.
10. Lusthaus, J. (2018). *Industry of Anonymity: Inside the Business of Cybercrime*. Harvard University Press. https://doi.org/10.2307/j.ctv24trdtf
11. Norton (2023). Cybercrime outlook 2023: It's all about the economy. https://us.norton.com/blog/emerging-threats/2023-predictions
12. SonicWall (2022). 2022 SonicWall Cyber Threat Report. https://www.sonicwall.com/resources/white-papers/2022-sonicwall-cyber-threat-report
13. Statista (2024). Cyber Crime & Security. https://www.statista.com/markets/424/topic/1065/cyber-crime-security/#overview
14. Verizon business (2024). Verizon's Data Breach Investigations Report. https://www.verizon.com/business/resources/reports/dbir/
15. Wall, D. S. (2007). Cybercrime: The Transformation of Crime in the Information Age. *Polity*. https://ssrn.com/abstract=1066922

Тютюник І., Топтуненко Д., Флаумер А.

КЛАСИФІКАЦІЯ СХЕМ КІБЕРЗЛОЧИННОЇ ДІЯЛЬНОСТІ: ОРГАНІЗОВАНА Й ТРАНСНАЦІОНАЛЬНА ЗЛОЧИННІСТЬ В ЕПОХУ ЦИФРОВИХ ТЕХНОЛОГІЙ

Метою цього дослідження є аналіз і класифікація основних схем організованої й транснаціональної кіберзлочинності, а також виявлення методів і технологій, які використовують кіберзлочинці для здійснення злочинної діяльності в цифровому просторі. У статті досліджені сучасні тенденції кіберзлочинності, такі як зростання фінансового шахрайства, атак програм-вимагачів, фішингу та DDoS-атак. Дослідження показує, що використання новітніх технологій, зокрема криптовалют та інтернету речей (IoT), значно ускладнює виявлення та притягнення до відповідальності кіберзлочинців, що зумовлює необхідність постійного вдосконалення правових і технічних засобів боротьби з кіберзлочинністю. Результати дослідження засвідчують, що транснаціональний характер кіберзлочинності часто ускладнює переслідування злочинців у різних юрисдикціях, що вимагає більшої міжнародної координації. Крім того, ускладнює процедури боротьби з кіберзлочинністю те, що вони використовують усе більш витончені методи приховування своєї діяльності, впроваджуючи сучасні технологічні рішення в злочинні схеми. Це підкреслює необхідність постійного моніторингу нових загроз і оновлення методів захисту й для організацій, і для окремих користувачів. У цілому, результати дослідження підкреслюють важливість глобальної співпраці в боротьбі з кіберзлочинністю, необхідність посилення технологічного захисту й розвитку правових механізмів протидії сучасним кіберзагрозам.

Ключові слова: організована й транснаціональна кіберзлочинність, фінансове шахрайство, атаки програм-вимагачів, фішинг, DDoS-атаки

JEL Класифікація: C38, F52, O17