CYBER RESILIENCE IN THE MODERN WORLD

CZU: 004.056:336.717
DOI: https://doi.org/10.53486/csc2025.17

MILLER CARINA
Academy of Economic Studies of Moldova
miller.carina@ase.md
ORCID ID: 0009-0006-6268-7081

Abstract. Cyber resilience is an essential aspect of modern cybersecurity strategies, ensuring the ability of organizations to anticipate, withstand, and recover from cyber threats. This paper explores the concept of cyber resilience in the context of increasing cyberattacks, particularly targeting financial institutions, government systems, and decentralized finance (DeFi) platforms. The research addresses key questions regarding the effectiveness of current cyber resilience frameworks and the role of emerging technologies such as artificial intelligence and blockchain in mitigating cyber risks. A mixed-method approach, combining statistical analysis of cyber incidents and expert interviews, was used to evaluate cyber resilience strategies. The results highlight the growing need for adaptive security measures, enhanced regulatory policies, and international cooperation. Data analysis suggests that organizations with proactive resilience strategies experience significantly lower financial losses and operational disruptions. The study concludes that cyber resilience should be a top priority for businesses and governments, requiring continuous improvement and investment in cybersecurity innovations.

Keywords: cyber resilience, cybersecurity, cyber threats, financial institutions, DeFi security, blockchain.

JEL Classification: L86, K24, O33

INTRODUCTION

Modern digital technologies have seriously changed the economy and public life. But along with new opportunities, new threats have emerged. One of them is cybercrime. Previously, these were mostly individual hackers, but now organized groups using sophisticated digital tools are increasingly operating.

Cryptocurrency has become one of the main tools of such criminal groups, as it can be used to conduct financial transactions anonymously. According to Chainalysis (2024), the volume of illegal cryptocurrency transactions in 2024 amounted to $40.9 billion, and this figure continues to grow. Cryptocurrency is actively used for money laundering and financing illegal activities.

It is becoming increasingly difficult to combat such crimes, especially due to the emergence of new technologies, such as artificial intelligence, blockchain analytics and anonymous networks. One example is Huione Guarantee, an illegal structure that was used for money laundering and fraud.

A research question: how does the corporate structure of cybercrime using cryptocurrencies affect the resilience of a digital society to cyber threats?

Theoretical basis:

– Theory of the digital economy (Tapscott & Tapscott, 2016)
– Theory of organized crime (Paoli, 2014)
– theory of cyber resilience (Linkov et al., 2019)

Hypothesis: digital criminal organizations using cryptocurrency technologies make it difficult to detect financial crimes and reduce the level of cyber resilience of society.

The purpose of the study is to track the development of cryptocrime, explore ways to counteract it and propose measures to improve digital security.

MAIN CONTENT

Modern cybercriminals are increasingly using advanced technologies to implement their schemes. The development of cryptocurrencies and anonymous networks such as Tor has given criminal groups more opportunities to hide their activities. This complicates the work of investigators and makes it more difficult to identify illegal transactions.

Cryptocurrencies such as Bitcoin and Ethereum were originally created as a means of decentralized exchange, but in practice they have become widely used in the shadow economy for money laundering, terrorist financing and other illegal purposes.

In recent years, criminals have increasingly switched to stablecoins, which are cryptocurrencies whose exchange rate is pegged to the dollar or another stable currency. This makes them less susceptible to price spikes. According to Chainalysis (2024), about 63% of illegal cryptocurrency transactions are accounted for by such stablecoins as Tether (USDT), USD Coin (USDC) and DAI. They are actively used in black markets, where it is important to reduce the risks associated with volatility.

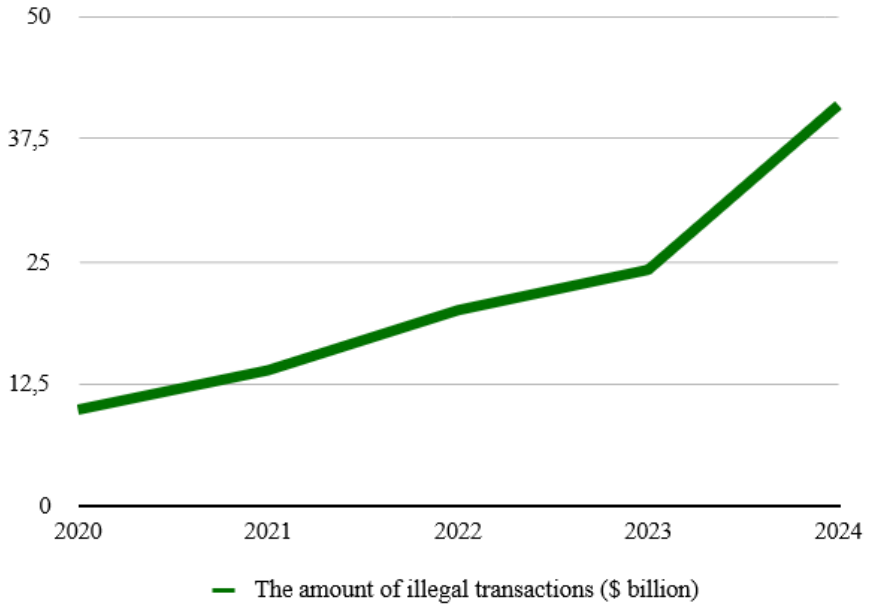

Figure 1. Growth in the volume of illegal cryptocurrency transactions from 2020 to 2024.
Source: *Chainalysis, 2024.*

In addition, the growing popularity of decentralized financial platforms (DeFi) poses a threat. Such platforms operate without control from centralized organizations, and their level of security is often low. In 2024, there were several major hacks of DeFi platforms, as a result of which more than 1.5 billion dollars were stolen. Criminals find vulnerabilities in smart contracts and withdraw funds so that they cannot be traced.

Cryptocurrency exchanges, which serve as the main source of liquidity, are also under attack. In 2024, hackers stole $2.2 billion from such platforms, which is 21% more than in the previous year.

The most commonly used method is to crack users' private keys, after which the attackers transfer funds to their wallets. Two-factor authentication and multi-signature are used for protection, but unfortunately not all users use these features, which makes them vulnerable.

In addition, artificial intelligence has also begun to be actively used in cybercrime. It creates adaptive viruses and Trojans that can change their structure depending on the protection systems. AI is also used for sophisticated phishing attacks — attackers create fake emails that look like real ones in order to lure people out of personal information. In 2024, the number of such attacks increased by 30%, which confirms the growth of digital risks.

Measures to Improve Cyber Resilience

To effectively combat cybercrime, a comprehensive approach is required, including international cooperation, the development of security technologies, legislative initiatives, and raising user awareness.

1. International Cooperation and Legal Measures:

Cybercrime requires global efforts. Organizations such as ENISA help countries exchange data and develop security standards. Significant steps also include international laws such as MiCA, which regulate cryptocurrency companies and prevent money laundering.

2. Security Technologies and Artificial Intelligence:

The use of machine learning and big data analytics allows for the rapid detection of transaction anomalies and fraud prevention. Blockchain technologies offer solutions to enhance transaction transparency and security. Implementing blockchain-based identification and multi-signature systems helps prevent unauthorized operations and increase trust in digital transactions.

3. Legislative Adaptation to New Threats:

It is essential to introduce laws regulating cryptocurrency operations, including mandatory transaction registration and exchange oversight. International coordination of such norms will help combat cybercrime.

4. Improving Digital Literacy and Awareness:

Educating users on online security, phishing detection, and personal data protection helps reduce attack risks. Awareness campaigns and cybersecurity training play a key role in protection.

CONCLUSIONS

This study examined the role of cryptocurrencies in the development of cybercrime and ways to improve the cyber resilience of the digital society. The results showed that cryptocurrencies, including stablecoins, are actively used for money laundering and criminal activity financing, making them a vital tool for criminal organizations. Notably, technologies such as blockchain and artificial intelligence play a key role in both criminal schemes and countermeasures against them.

The proposed methods for enhancing cyber resilience, including international cooperation, security technology development, legislative adaptation, and user awareness, emphasize the importance of a comprehensive approach to combating cyber threats. However, several unresolved issues remain, such as the need for further improvement of cryptocurrency legislation and the search for new solutions to counter transaction anonymity.

This study opens new directions for further research, which should focus on a deeper analysis of specific cases of cryptocurrency use for criminal purposes and the assessment of the effectiveness of proposed measures. Future research should also address differences in cryptocurrency regulations across countries and explore innovative solutions for ensuring the security of digital transactions.

REFERENCES

1. Chainalysis. “2024 Crypto Crime Report.” Chainalysis, 2024. Available at: https://www.chainalysis.com/blog/2025-crypto-crime-report-introduction/
2. Financial Times. “North Korean Lazarus Group and Global Crypto Heists.” Financial Times, 2024. Available at: https://www.ft.com/content/4ed7ce45-a653-496e-99a6-ade9c21f9908 [Accessed 24.02.2025].
3. El País. “Stablecoins and Their Role in Illicit Transactions.” El País, 2024. Available at: https://english.elpais.com/economy-and-business/2025-01-05/the-new-gray-area-dollar-in-venezuela-is-digital.html [Accessed 24.02.2025].
4. Reuters. “Rise in Crypto Exchange Hacks in 2024.” Reuters, 2024. Available at: https://www.reuters.com/technology/losses-crypto-hacks-jump-22-bln-2024-report-says-2024-12-19/ [Accessed 24.02.2025].
5. Europol. “AI and Cybercrime: Emerging Threats.” Euronews, 2024. Available at: https://www.euronews.com/next/2024/10/02/ai-is-making-cyberattacks-more-sophisticated-and-cybersecurity-teams-are-struggling-to-kee [Accessed 24.02.2025].