The impact of cyberattacks on the stability of global financial markets as a manifestation of economic terrorism

Marcin Surówka[1], Zbigniew Małodobry[2], Karolina Nastaj-Sałek[3], Katarzyna Cyrkun[4]

[1]Cracow University of Economics
Poland

[2]University of Rzeszów
Poland

[3]State Vocational University of prof. Stanisław Tarnowski in Tarnobrzeg
Poland

[4]Military University of Technology
Poland

***Abstract*— The article conducts a comprehensive analysis of the impact of cyberattacks on global financial markets, focusing on their characterization as a form of economic terrorism. Various types of cyber threats were discussed, including DDoS attacks, malware infections, phishing techniques and ransomware, highlighting their ability to immediately and long-term destabilize financial institutions. The immediate effects of such attacks include financial disruption, severe financial losses and data theft, which directly impacts customer and investor confidence. The authors analyze in detail the indirect effects of cyberattacks, pointing to a decrease in trust in financial systems, which may lead to the withdrawal of capital and a decline in investment activity on the markets. Moreover, the need to increase investment in security technologies and the development of advanced defense strategies increases the operating costs of financial institutions. The article also highlights the growing threat of cyberterrorism, identified as organized cybercriminal or state-led activities aimed at spreading fear and uncertainty, resulting in long-term socio-economic impacts. In the context of countering threats, the article recommends tightening international cooperation in monitoring and responding to cyber threats. Moreover, exchanging information about threats and best cybersecurity practices is crucial for effective defense against cyberattacks.**

Keywords— new technologies, cyberwar, cyberterrorism, economy, financial market, security.

I. INTRODUCTION

Modern financial markets, characterized by high complexity and global integration, are a key element in the functioning of economies around the world. For this reason, they are particularly susceptible to various threats - including those resulting from the development of information technologies. In recent years, cyberattacks have become one of the most serious challenges to the stability of global financial markets. These attacks, which use advanced hacking techniques and malware, can lead to serious disruptions in the operations of financial institutions, data loss and a decline in investor and customer confidence.

It is worth noting that cyberattacks on financial markets may be perceived as a form of economic terrorism, where the goal is not only to achieve direct financial benefits, but also to destabilize national and global economies. Economic terrorism through cyberattacks is becoming a tool used by terrorist groups and states pursuing hostile policies that seek to weaken their opponents by destroying their economic sectors. In the face of the growing number and scale of these attacks, analyzing their

ASEJ - Scientific Journal of Bielsko-Biala School of Finance and Law
Volume 28, No 2 (2024), pages 4
https://doi.org/10.19192/wsfip.sj2.2024.6
Received: March 2024 Accepted: May 2024
Published: June 2024

impact on the stability of financial markets and developing effective defense and prevention strategies is becoming an essential element of contemporary economic security policy.

The aim of this work is to thoroughly examine the impact of cyberattacks on the stability of global financial markets, with particular emphasis on aspects related to economic terrorism. This work aims not only to present the mechanisms of action and effects of cyberattacks, but also to identify effective methods of protection against them and discuss the role of international cooperation in combating this type of threats. The first part of the work will discuss the basic concepts and types of cyber attacks, and then analyze specific cases of attacks on financial institutions. The preventive measures and defense strategies used by financial institutions and governments will be presented in turn. Finally, the work will present future challenges and development prospects in the context of protecting financial markets against cyberattacks.

II. CYBERTERRORISM

First of all, it is worth defining the concept of cyberterrorism. Experts point out the difficulties associated with clearly defining this term, which makes the identification of activities qualifying as cyberterrorism complicated. Barry Collin from the Institute for Security and Intelligence in California is considered the creator of the term "cyberterrorism", who used it in the 1980s to describe the combination of cyberspace and terrorism (Denning 2002, p.79).

Cybercrime is increasingly perceived as a manifestation of terrorism, especially in the context of its impact on the stability and security of global financial markets and the broader economy. Cyberterrorism refers to intentional and organized activities intended to disrupt, destroy, or manipulate computer systems, networks, and critical infrastructure to achieve political, ideological, or social goals. Unlike traditional cybercrime, motivated mainly by financial gain, cyberterrorism aims to cause fear, chaos and destabilization of societies and states (Wiśniewski, Boehlke 2016).

One of the main targets of cyberterrorism are financial institutions, which constitute the backbone of the modern economy. Attacks on banks, stock exchanges and payment systems can lead to serious disruptions in the functioning of financial markets, causing wide-ranging economic consequences. An example is a DDoS attack on banks, which may paralyze their activities, preventing transactions and causing loss of trust among customers and investors (Ibidem).

Cyberterrorism is not limited to financial institutions. Attacks on critical infrastructure such as energy networks, transport and communication systems can also indirectly impact financial markets, leading to widespread economic losses and social destabilization. For example, an attack on the power grid could paralyze stock exchanges, preventing transactions and causing chaos in financial markets.

With the growing threat of cyberterrorism, close cooperation between financial institutions and governments around the world is essential to develop effective defense strategies. It is crucial to invest in advanced security technologies such as artificial intelligence and blockchain that can effectively detect and neutralize threats. International cooperation and exchange of information are equally important, which enables quick response to new threats and sharing of best practices (Nowalska-Kapuścik 2017, p. 138).

D. Denning proposes a more precise definition of cyberterrorism, defining it as an unlawful attack or threat of attack on computers, networks or information systems, intended to intimidate or enforce far-reaching political and social goals. According to Denning, an act of cyberterrorism must cause direct harm to people and property or be serious enough to cause fear (Denning 2000, p. 45).

Cyberterrorism, as a specific category of threats, includes activities directed against ICT systems aimed at achieving specific terrorist goals. Types of cyberterrorism can be distinguished based on subjective and objective criteria. From the perspective of the subjective criterion, cyberterrorists and their victims are taken into account, i.e. the entities that carry out the attacks and those that are their targets. In the context of international relations, victims of attacks can be both state and non-state actors. The perpetrators include organized groups and individual cyberterrorists (Maj 2001, p. 15).

Organized cyberterrorist groups include both classic terrorist organizations, such as the Tamil Tigers, Hezbollah and Al-Qaeda, which, in addition to traditional methods, also use cyberspace, as well as groups consisting of computer hackers operating almost exclusively in cyberspace. Individual cyberterrorists, in turn, are specialized units whose activities are commissioned by terrorist organizations for an appropriate fee.

The objective criterion refers to the effects of cyberterrorist attacks, which may be of a military, economic and political nature. An example of military consequences is the activity of hackers hired by the Chinese authorities, who in the late 1990s stole secret information from the nuclear weapons research laboratory in Los Alamos in New Mexico. This case, revealed in 2000, showed that China obtained information about every American nuclear warhead.

III. CYBER-ATTACKS - CHARACTERISTICS AND TYPES

In the context of the stability of global financial markets, it is crucial to understand the different types of cyber attacks in order to assess potential threats and develop effective defense strategies. DDoS (Distributed Denial of Service) attacks involve overloading networks, servers or target services with huge amounts of Internet traffic, which leads to their overload and prevents normal functioning. In the case of financial markets, DDoS attacks may cause downtime in the operations of banks, stock exchanges and other financial institutions, resulting in serious financial losses and loss of customer trust (Dziamdziora 2021, p. 13).

Malware includes a variety of programs such as viruses, trojans, worms, ransomware, spyware and adware. Malware can be used to steal data, destroy files, take control of computer systems, or extort ransoms to unlock infected devices. In the

financial sector, malware can be used to steal confidential information such as customer data, passwords, credit card numbers and to conduct unauthorized transactions.

Phishing is a method of fraud that involves impersonating trusted entities in order to obtain confidential information, such as login details, credit card numbers or other personal data. Phishing attacks are often carried out using fake emails, SMS messages or websites that appear authentic. In the financial sector, phishing may lead to unauthorized access to bank accounts, identity theft and other forms of financial fraud (Wrona 2020, pp. 57-63).

Ransomware is a type of malware that encrypts files on an infected computer or an entire network and then demands a ransom to restore access to the locked data. In the context of financial institutions, ransomware attacks can paralyze operations by preventing access to critical data and systems, which can lead to significant business disruptions and financial losses. An example of a significant ransomware attack is the attack on the British NHS in 2017, which caused chaos and significant financial losses.

Advanced and sustained attacks, known as APT (Advanced Persistent Threat), are carried out by well-organized cybercriminal or state-sponsored groups. APTs are characterized by long-term planning and targeted action aimed at gaining access to the victim's network and remaining there for a long time without detection. In the case of financial institutions, APTs can be used to steal confidential information, such as transaction data, strategic plans or trade secrets (Bowdur, Aptekorz 2014, p. 70).

SQL Injection attacks involve injecting malicious SQL code into database queries. These types of attacks can lead to unauthorized access to data, modification of the database or its deletion. In the financial sector, SQL Injection attacks can be used to steal customer data, change bank account balances, or other forms of fraud (Evien, Hanselman, Rader 2014, p. 1729).

Man-in-the-Middle (MitM) attacks involve intercepting and modifying communications between two parties without their knowledge. An attacker can intercept login credentials, financial information, or other confidential information sent between the user and the server. In the financial sector, MitM attacks can lead to data theft, financial fraud and loss of customer trust.

IV. THE IMPACT OF CYBERATTACKS ON THE STABILITY OF GLOBAL FINANCIAL MARKETS

Cyberattacks are increasingly affecting the stability of global financial markets, posing a serious threat to their functioning and integrity. These markets, characterized by high complexity and global integration, are particularly vulnerable to cyber attacks, which may result in serious operational disruptions, financial losses and loss of investor and customer confidence (Michael 2017, p. 16).

The immediate consequences of cyberattacks include disruptions to the operations of financial institutions such as banks, stock exchanges and payment systems. DDoS attacks can overload servers, making them unavailable and making financial transactions impossible. Malware and ransomware can infect computer systems, blocking access to key data and systems, paralyzing operations and requiring large investments to restore normal functioning. However, phishing attacks and other forms of identity theft allow cybercriminals to gain unauthorized access to confidential information, which can lead to serious financial losses (Ibid).

The indirect consequences of cyberattacks are also significant. These include decreased investor and customer confidence in financial institutions, which may result in the withdrawal of funds and a decline in investment activity. Financial institutions may also need to increase investment in security technologies and the development of advanced defense strategies, which increases their operating costs. Additionally, in response to the growing threat of cyberattacks, governments and regulatory authorities may introduce more stringent cybersecurity regulations, which further increases the costs and operational complexity of financial institutions (Mądrzejowski 2008, p. 56).

Examples of significant cyberattacks on financial institutions, such as the attack on JPMorgan Chase in 2014 and the attack on the SWIFT system in 2016, illustrate the seriousness of the effects of these incidents. The attack on JPMorgan Chase led to the theft of the personal data of millions of customers, which resulted in significant financial losses and a serious reduction in customer confidence. However, the attack on the SWIFT system, used for international financial transfers, showed that even the most advanced systems can be susceptible to cyber threats, which has a direct impact on global financial flows.

In response to these threats, financial institutions must constantly develop and update their cybersecurity strategies, investing in modern technologies such as artificial intelligence and blockchain that support the detection and neutralization of threats. International cooperation is also crucial, enabling the exchange of information on threats and best practices in the field of protection against cyberattacks.

V. CONCLUSIONS

The impact of cyberattacks on the stability of global financial markets as a manifestation of economic terrorism is a complex and multi-faceted challenge that requires a comprehensive approach and coordinated actions on many fronts. Financial markets, characterized by a high degree of globalization and technological complexity, are particularly susceptible to cyber threats that can lead to serious operational disruptions, financial losses and loss of investor and customer confidence (Michael 2017, p. 16).

The immediate effects of cyberattacks include disruptions to the operations of financial institutions such as banks, stock exchanges and payment systems. DDoS attacks can overload servers, preventing financial transactions from being completed, while malware and ransomware can block access to key data and systems, paralyzing operations. Phishing attacks

and identity theft can lead to unauthorized transactions and serious financial losses (Ibid).

The indirect consequences of cyberattacks are equally important. They include, among others: decreased trust in financial systems, which may result in the withdrawal of funds and a decline in investment activity. Financial institutions are forced to increase investment in security technologies and develop more advanced defense strategies, which generates additional operational costs. Additionally, the growing threat of cybercrime requires more stringent regulations, which increases operational complexity and compliance costs (Mądrzejowski 2008, p. 56).

In the context of economic terrorism, a cyber attack becomes a tool for causing widespread disruption and destabilization. Cyberterrorists, often acting on behalf of states or extremist organizations, use advanced technologies to carry out coordinated attacks. Their goal is not only to cause direct financial losses, but also to spread fear and uncertainty, which leads to long-term socio-economic consequences. Examples of attacks on critical infrastructure, such as energy networks or transport systems, illustrate the potential of cyberterrorism to paralyze economic sectors and destabilize global financial markets.

An effective response to these threats requires coordinated action at many levels. Financial institutions should invest in modern security technologies, such as artificial intelligence and blockchain, that enable quick detection and neutralization of threats. International cooperation in monitoring and responding to cyber threats is also key. International organizations and government agencies should intensify the exchange of information on threats and best practices in the field of cybersecurity.

Education and public awareness are key to building resilience to cyber threats. Training of employees of financial institutions and education of customers are necessary to increase awareness of digital threats and enable effective response to incidents.

To sum up, the impact of cyberattacks on the stability of global financial markets as a manifestation of economic terrorism is a serious challenge that requires a comprehensive approach. Financial institutions, governments and the international community must cooperate by investing in modern technologies, developing defense strategies and educating the public. Only then will it be possible to ensure the stability and security of global financial markets in the face of growing cyber threats. Further technological innovations are expected in the future, which will both accelerate the development of global financial markets and increase their exposure to cyber threats. With the development of artificial intelligence, the Internet of Things and blockchain technology, the potential for both cybercriminals and financial institutions to ensure security is growing. The key challenge will be not only the response to existing threats, but also the ability to anticipate new types of attacks and quickly adapt to the changing cybersecurity landscape.

VI. REFERENCES

Bowdur E., Aptekorz M. (2014), Selected issues and trends of contemporary digital education, Stowarzyszenie Komputer i Sprawy Szkoły, Mikołów.

Denning D. E. (2000), Cyberterrorism. Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives, Washington.

Denning D. E. (2002), Wojna informacyjna i bezpieczeństwo informacji, Warszawa.

Dziamdziora W. (2021), Cyberbezpieczeństwo w samorządzie terytorialnym. Praktyczny przewodnik, Wolters Kluwer, Warszawa.

Evien B., Hanselman S. Rader D. (2014) ASP.NET 3.5 z wykorzystaniem C# i VB. Zaawansowane programowanie, Helion, Gliwice.

Maj P. (2001), Cyberterroryzm w stosunkach międzynarodowych, „Consensus. Studenckie Zeszyty Naukowe", no. 1.

Mądrzejowski W. (2008), Przestępczość zorganizowana. System zwalczania, Wydawnictwa Akademickie i Profesjonalne, Kraków.

Michael R., Managing Media Businesses (2017), A Game Plan to Navigate Disruption and Uncertainty, Sprinter Science + Business Media, New York.

Nowalska-Kapuścik D. (2017), Technologia jako inspiracja dla interdyscyplinarnych badań naukowych, e-bookowo, Będzin.

Wiśniewski P., Boehlke J. (2016), Cyberprzestępczość w gospodarce, Wydawnictwo Naukowe Uniwersytetu Mikołaja Kopernika, Toruń.

Wrona J. (2020), Cyberprzestrzeń a prawo międzynarodowe. Status quo i perspektywy, Wolters Kluwer, Warszawa.