ACIG
APPLIED CYBERSECURITY & INTERNET GOVERNANCE

NASK

Assessment of the Cybersecurity of Ukrainian Public Companies Listed on the Warsaw Stock Exchange S.A.

Anna Szczepańska-Przekota | Department of Finance, Faculty of Economic Sciences, Koszalin University of Technology, Poland | ORCID: 0000-0002-4002-5072

Abstract

Nowadays, the number of sophisticated cyberattacks targeting critical infrastructure or banking systems is increasing. Cases of successful attacks are not uncommon, as statistics in Ukraine demonstrate, and they are becoming more frequent and advanced. This results in an increased risk for companies listed on the stock exchange. The article provides examples of cyberattacks in Ukraine, including those using ransomware, attempts to infiltrate energy systems, and attacks on government institutions. It is noted that the presence of cyber threats is strongly linked to the political and international situation of the country. Analyses conducted focus on the examination of cyber threat events in Ukraine and their impact on the WIG_UKRAIN stock index from 2015 to 2023. The evaluation includes the index's return rates on the day of the cyber threat occurrence, the following day, and the average return rate within five sessions after the threat. An analogous study for the WIG index is adopted as a benchmark. Based on the obtained results, it can be said that before the year 2022, cyberattacks on Ukraine did not have a significant impact on the value of the Ukrainian company stock index. The situation changed after 2022, where each potentially economically harmful cyberattack contributed to the decrease in the value of Ukrainian-listed companies. Generally, the start of hostilities in 2022 significantly increased the volatility of the WIG_UKRAIN index quotations. This is to be expected, as markets react badly to uncertainty.

Received: 25.02.2024

Accepted: 22.05.2024

Published: 15.07.2024

Cite this article as:
A. Szczepańska-Przekota "Assessment of the cybersecurity of Ukrainian public companies listed on the Warsaw Stock Exchange S.A.," ACIG, vol. 3, no. 1, 2024, DOI: 10.60097/ACIG/190343

Corresponding author:
Anna Szczepańska-Przekota, Department of Finance, Faculty of Economic Sciences, Koszalin University of Technology, Poland.
E-mail: anna.szczepanska-przekota@tu.koszalin.pl;
0000-0002-4002-5072

Keywords
cybersecurity, cyberspace, cyber threat, WIG_UKRAIN index, WIG index

1. Introduction

The sectors of the economy, such as transportation, energy, healthcare, and finance, are becoming increasingly dependent on digital technologies in their core activities. The digital era creates vast opportunities and brings unparalleled economic growth, connecting businesses worldwide and supporting innovation. However, these interconnections have also exposed organisations and society to a constant threat of cyberattacks.

Cyberattacks are becoming more frequent and sophisticated throughout Europe. The surge in ransomware and cyberattacks increased by over 150% throughout the entirety of 2020. This signifies that cyber insurance is becoming a less profitable business for insurers [1]. According to forecasts, by 2025, as many as 41 billion devices worldwide will be connected to the Internet of Things. Therefore, decisive actions towards cybersecurity can enhance the credibility of digital tools and services, primarily ensuring the security of businesses operating in a cyber environment on a daily basis.

Ukrainian publicly traded companies, like many others worldwide, face the challenge of navigating the complex landscape of cybersecurity. The article presents the cybersecurity landscape of Ukrainian publicly traded companies, examining the threats they face, the measures they take, and the need for constant vigilance in the digital age.

The conducted analysis covers specific cases of cyberattacks, their complexity, economic consequences, and the financial market's response. The overview of events underscores the role of geopolitical situations in shaping the market's sensitivity to cyber threats. The ultimate aim is to provide a comprehensive understanding of how cyber threats impact the stock value of Ukrainian companies and to indicate potential remedial actions for businesses facing increasing cyber risks.

1.1. The Essence of Cybersecurity and Cyber Threats

In today's world, where technology plays a crucial role in all aspects of life, cybersecurity is becoming increasingly important for individuals, businesses, institutions, and nations seeking to

effectively protect their digital assets from threats. It is worth noting that security is perceived as an objective state, characterised by the absence of threat, subjectively felt by individuals and groups [2]. In common understanding, security may denote a state in which an individual has a sense of certainty in a smoothly functioning legal and economic system. Security should not be treated as an independent variable, as it has a dynamic nature and can change due to complex phenomena [3].

Cybersecurity involves the resilience of information systems against actions that violate the confidentiality, integrity, availability, and authenticity of processed data or related services offered by these systems. The goal of cybersecurity is to secure information technology (IT) infrastructure, software, personal data, and ensure the integrity, availability, and confidentiality of information.

The communication space created by Internet-related linkages (cyberspace) is where processes threatening security are embedded. Cybersecurity threats are potential causes of incidents, and the vulnerability of an IT system is a characteristic that can be exploited by cybersecurity threats. According to the definition formulated by the US Department of Defense, cyberspace is a 'global domain within the information environment consisting of the interdependent networks of information technology infrastructure (IT) and data contained therein, including the Internet, telecommunication networks, computer systems, and embedded processors and controllers' [4]. Thus, cyberspace constitutes a kind of communication space created by Internet-related linkages [5]. Analysing the features of this cyber space indicates that it is a unique techno-system of global social communication, shaped by the integration of forms of information transmission and presentation, leading to digitalisation and the creation of a global integrated teleinformatics platform [6].

The opposite of security is a state of threat, the nature of which is associated with an objective category of risk that always exists independent of human awareness. Awareness of threat becomes a key decision criterion in every area of human and economic entity functioning, subject to management [7]. In the literature of economics and finance, risk is defined differently [8, 9]. Events in the geopolitical sphere confirm that risk is embedded in a dynamic evolutionary model of the world. Risk is associated not only with the realisation of specific intentions but also with the desire to maintain the existing state of affairs, that is, not taking or refraining from certain actions [10].

It is different from uncertainty, which relates to events or changes that are difficult to estimate, and the probability is completely unknown [11]. This phenomenon has caused the number and severity of cyber threats in recent years to be unprecedented, and the costs of cyberattacks for corporate boards and other external and internal stakeholders are enormous. The consequences caused in cyberspace by unauthorised users lead to dangerous social and economic consequences. Institutions and companies are taking initiatives to protect data, critical business processes, and the availability and integrity of information systems. The constantly evolving cyber threats, including those related to the armed conflict in Ukraine and the recent acceleration of digitisation, are key factors driving the need to develop appropriate tools to increase organisations' capabilities in managing cybersecurity risk [12]. It is believed that cybersecurity needs to be incorporated at all levels of the company's business model, that is, both in operational and supporting processes.

In Poland, a significant legal act regulating aspects of cybersecurity is the Act on the National Cybersecurity System. According to the Security Strategy of the Republic of Poland for the years 2019–2024, a cybersecurity threat is any potential circumstance, event, or action that may cause harm, disruption, or otherwise adversely affect networks and teleinformatic systems, users of such systems, and other individuals, in accordance with the Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on the European Union Agency for Cybersecurity (ENISA) and on cybersecurity certification of Information and Communication Technology (ICT) products and repealing Regulation (EU) No. 526/2013 (the Cybersecurity Act).

According to the Threat Landscape Report – 2021 (ENISA Threat Landscape – 2021), the most significant cyber threats include the following:

- ransomware software,
- malicious software (malware),
- email-related attacks,
- threats related to data,
- threats related to availability and integrity,
- disinformation.

Vulnerability to cyberattacks is an objectively defined probability that the security system of an enterprise may be threatened. This indicates the likelihood of exploiting a gap in a specific security

system. Refsdal et al. argue that cyber risk is not synonymous with every risk to which a cyber system may be exposed; cyber risk is limited to the risk caused by cyber threats [13].

The risk of server damage, such as flooding, is not a risk associated with cyberspace unless facilitated by a cyber threat. Examples of cyber threats include breaches of confidentiality through virus attacks in cyberspace and loss of availability due to denial-of-service (DoS) attacks.

The cybersecurity risk of an enterprise depends on various internal and external factors, including the size of the company's assets, the technology it employs, vulnerability to threats, awareness and competence of employees in security matters, cybersecurity procedures, supplier (outsourcing) security, the vulnerability of the overall infrastructure on which the enterprise operates, and the motivation of potential criminals. Considering all these factors and the limited knowledge about the impact of individual factors on the overall enterprise risk, understanding, and estimating cyber insurance risk is very complex. Simple metrics, such as the number of lost records, do not always correlate with the total cost of risks [14].

1.2. Cybersecurity Challenges in Ukraine

Ukraine, emerging as an economic powerhouse in Eastern Europe, boasts a growing number of companies listed on stock exchanges. However, the country's geopolitical situation has made it a primary target for cyberattacks. The ongoing conflict with Russia, which began in 2014, has complicated Ukraine's cybersecurity landscape. Cyberattacks, often attributed to state-sponsored entities, target critical infrastructure, government agencies, and private sector entities.

Ukrainian publicly traded companies may be particularly vulnerable to these threats. They must confront a series of cybersecurity challenges, such as the following:

- Phishing attacks, where cybercriminals use deceptive email messages and fake websites to persuade employees to disclose confidential information or install malicious software.
- Ransomware attacks crippling operations and demanding high ransoms.
- Vulnerabilities in supply chain security, as globalised companies rely on international supply chains, and cyberattacks on

partners or suppliers can have a cascading impact on Ukrainian enterprises.
- Politically motivated state-sponsored attacks that can result in significant financial damages.
- Internal threats where employees may intentionally or unintentionally breach cybersecurity measures.

Ukraine has experienced various forms of cybercrimes, both related to the conflict with Russia and stemming from the overall rise in global cyber threats. These include hacking attacks on critical infrastructure, attempting to infiltrate energy systems, telecommunications, or air traffic management systems. Such attacks can have serious consequences for public safety and the functioning of the state. Another form of cybercrime is data theft and attacks on government institutions, where hackers seek illegal access to sensitive data, such as citizens' personal information or classified government data. These attacks may be politically motivated, aiming to acquire confidential information or spread disinformation.

Financial systems are common targets for cybercriminals attempting to infiltrate banks and financial institutions to steal funds or manipulate financial systems. Ransomware attacks follow a similar pattern, infecting computer systems or networks and then demanding ransom in exchange for restoring access to data or systems. Companies, public institutions, and administrative entities may be targeted in such attacks. Attacks on the educational sector, such as schools, universities, and other educational institutions, are also prevalent due to the sensitive personal data of students and employees they store.

The Ukrainian government is taking actions to secure against these threats, but new cybercriminal techniques continue to emerge. Therefore, education, international collaboration, and continuous security system updates are crucial in combating these types of threats.

The extent and capabilities of non-state cyber actors became evident primarily during the Russian-Ukrainian war. According to Štrucl [15], the Russian Federation's previously successful hybrid warfare strategies faced challenges in the initial months of the 2022 war due to the active involvement of various hacking and hacktivist groups aligning themselves with the conflict. In the Ukrainian context, there seems to be an unspoken agreement among state institutions to allow non-state cyber actors to selectively carry out cyber defence functions. In February 2022, Ukrainian Deputy

Prime Minister M. Fedotov advocated for the establishment of the Information Technology Army of Ukraine. Hacktivist groups, such as Network Battalion 65, Elves, Cyber Guerrillas, Cloud Atlas, and notably, Anonymous, have been engaged in anti-Russian and anti-Belarusian activities, with Anonymous emerging as the most media-savvy cyber participant in the conflict [16].

1.3. Enhancing Cybersecurity Measures

In response to these threats, Ukrainian publicly traded companies increasingly recognise the importance of robust cybersecurity measures. Several strategies are employed to protect digital assets:

1. Organisations develop comprehensive cybersecurity policies and provide training to employees to raise awareness and promote best practices in cybersecurity.
2. Utilising high-quality software on end-user workstations, such as Endpoint Detection and Response (EDR) systems, helps secure and monitor computers, servers, and smartphones within the organisation. If any point in the IT system is infected, it is immediately isolated to prevent the attack from spreading to the entire corporate network and other devices.
3. Investments in advanced firewalls, intrusion detection systems, and endpoint protection are essential for safeguarding against cyber threats.
4. Developing and testing incident response plans is crucial for minimising the damage resulting from cyberattacks.
5. Companies conduct regular security audits and vulnerability assessments to identify and address weak points.
6. Collaborating with Ukrainian law enforcement and international partners can assist in effectively tracking and responding to cybersecurity threats.
7. Investing in employee education has a positive impact on the company's security levels. Hackers often initiate attacks by sending messages to ordinary employees, because there is a significant chance that such a person will click on an infected link. Awareness of cyber threats among employees varies and is usually lower than that of IT specialists. Regular training sessions enable the elevation of knowledge levels and the adoption of best practices, enhancing employees' resilience to hacker manipulations.

While these measures are essential, it is crucial to remember that the cybersecurity landscape is constantly evolving. Cybercriminals continuously develop new tactics and exploit vulnerabilities,

requiring companies to maintain adaptability and vigilance. A proactive approach to cybersecurity is the most effective way to anticipate potential threats. Companies must also be aware of the regulatory environment. The Ukrainian government is working on cybersecurity regulations to strengthen legal frameworks for cybersecurity and data protection. Adhering to these regulations is not only a legal requirement but also a prudent cybersecurity practice.

Many studies show that cyberattacks, especially those directly targeting listed companies, cause significant damage [17]. This damage spreads throughout the industry [18]. As a result, investor confidence in such companies declines, the share price and hence the market value of the company falls, and share price volatility increases. There is usually a negative market reaction immediately after the attack [19]; the markets do not wait for the effects of such attacks to be determined. These are all negative phenomena. There is no positive market reaction to cyberattacks. In the long run, the situation can go one of the two ways: if the company tries to counter the attack, it can stay in the market [20]; technology companies are usually better prepared for attacks than companies in other industries [21]; if it does not take action, then it risks being taken out of the market [22].

2. Methods

The subject of the study is cyber threat events in Ukraine and their impact on the quotes and returns of the WIG_UKRAIN index during the period from December 2015 to December 2023 on the Warsaw Stock Exchange (GPW) S.A. Analyses conducted focus on the examination of cyber threat events in Ukraine and their impact on the WIG_UKRAIN stock index from 2015 to 2023. The evaluation includes the index's return rates on the day of the cyber threat occurrence and the average return rate within sessions after the threat. According to the efficient market hypothesis, any event that could affect the valuation of financial instruments is discounted in the market price. Cyber threats are considered information that could potentially influence the value of financial instruments. Of course, cyber threats vary in type and scope of impact. Therefore, a review of selected cyber threats was conducted, and an assessment of their impact on the value of the Ukrainian companies' index was made. The returns of the index were observed on the following events:

1. The day of the cyber threat occurrence.
2. The day immediately following the cyber threat occurrence.
3. The average return over five sessions following the cyber threat occurrence.

The performance of the WIG stock index was chosen as a reference point, for which corresponding returns were determined. During the period under review, the average volatility of the WIG_UKRAIN index quotations was compared with the WIG index quotations. Low rates of return were considered as the negative effect of reducing the value of Ukrainian-listed companies as a result of cyber activities. The WIG-Ukraine index is the second national index calculated by the stock exchange. It includes companies listed on the Warsaw Stock Exchange (GPW) whose headquarters or central offices are located in Ukraine or whose activities are predominantly conducted in this country. The first value of the index was published on 4 May 2011. Historical values of the index were recalculated from the base date of the index, which is 31 December 2010, when the index value was 1000 points. WIG-Ukraine is an income index, considering both prices of the stocks included and income from dividends and rights issues in its calculation.

On the other hand, the Warsaw Stock Exchange Index (WIG) encompasses stocks of companies listed on the primary market. It is the longest-standing index on the Warsaw Stock Exchange (GPW), calculated since 16 April 1991. WIG is an income-type index, meaning that its calculation takes into account both prices of the stocks included and income from dividends and rights issues. It also expresses the relative total value of the companies present on the Warsaw Stock Exchange (GPW) in relation to their value at the beginning of the index listing.

The main limitation of the research is the difficulty in determining the date of publication of information about a cyberattack. Several key dates there: the date of preparation of the cyberattack, the date of the cyberattack, the date of information about the cyberattack, and the date of reaching the market. Each of these dates is critical, but none can be determined with complete accuracy. It is often necessary to act on the basis of residual information. In addition, the number and nature of all cyberattacks are not known, so it is necessary to focus on a few.

3. Results

The onslaught of attacks on information systems using malicious software, such as ransomware, is immense, and furthermore, the size of the hacker arsenal is increasing. History shows that the actions of cybercriminals vary depending on the political, economic, and international situation in Ukraine. In most cases, these actions aimed to acquire confidential information related to Ukraine's politics, defence, or economy.

3.1. Examples of Cyberattacks on Ukraine

Examples of cyberattacks have been compiled in Table 1.

Table 1. Examples of cyberattacks on Ukraine.

Date	Type of threat	Consequences
23 December 2015	• Attacks on the energy sector – APT Sandworm.	• Power outages affecting approximately 230,000 consumers for 1–6 h. • Preventing customers from calling to report emergencies – malfunction of 16 telephone line substations. • Attempt to undermine trust in Ukrainian energy companies and the government.
17 December 2016	• Before the cyber incident, cybercriminals conducted a 'denial of service' phone attack on customer service centres.	• Over an hour-long blackout. • Power outage led to the loss of about one-fifth of energy consumption in Kyiv at that time of night. • Disruption of power distribution, cascading failures, and equipment damage.
23 & 28 December 2016	• Malicious software. The Security Service of Ukraine (SBU) apprehended Russian special service officers who attempted to damage a series of computer networks in infrastructure facilities in Ukraine.	• SBU discovered malicious software on the computers of regional operators of power grid networks. The virus attack was coordinated with a flood of phone calls to the hotline of several energy companies.
27 July 2017	• Attack on public, financial, and energy sectors. • Attack using malicious software for data erasure, known as NotPetya. The attack is described as the 'most destructive cyberattack in history'.	• The radiation monitoring system at the Ukrainian nuclear power plant in Chernobyl was shut down. • Economic loss for Ukrainian entities due to irreversible data encryption. • Infiltration of computer networks, including systems of the National Bank of Ukraine, Kyiv-Boryspil International Airport, and the capital's metro. • Affected 65 countries and approximately 49,000 systems worldwide. • Estimated global economic losses exceeding US$10 billion.
11 July 2018	• 'VPN Filter' attack on the chlorine distillation system.	• Cyberattack on the network devices of the Chlorine Distillation Station in Auly, which supplies liquid chlorine to water and sewage treatment plants in 23 provinces of Ukraine as well as Moldova and Belarus.
13 January 2022	• Virus attacks (ransomware) erasing data, known as 'WhisperGate', targeting all sectors of the economy.	• Microsoft has identified a destructive operation of malicious software (labelled as WhisperGate) targeting multiple organisations in Ukraine. It is designed to appear as ransomware, but lacks a ransom recovery mechanism and is intended for the destructive shutdown of targeted devices, rather than extortion. The victims include various government, non-profit, and IT organisations.

(*continues*)

Table 1. Continued.

Date	Type of threat	Consequences
14 &15 January 2022	• Hacker attack on government websites, Ministry of Education, State Emergency Service, government, Ministry of Energy, and the government application Dija, which allows for the use of documents in digital form and access to some public services. • Alteration of content on government websites – Belarus APT Group – UNC1151.	• Because of the attack, government websites temporarily ceased to function. The goal was data cleansing. • The attack paralysed a significant portion of the government's digital public infrastructure, including the most frequently used website for handling online government services, Diia. Diia also plays a role in responding to the coronavirus in Ukraine and encouraging vaccinations. The application also disabled the headquarters of the cabinet of ministers, ministries of energy, sports, agriculture, veterans affairs, and ecology.
15 & 16 February 2022	• Distributed denial-of-service (DDoS) attack on websites of financial and public sectors. • DDoS attack described as the largest to date in Ukraine.	• At least 10 Ukrainian websites were inaccessible, including the Ministry of Defence, Ministry of Foreign Affairs, and two largest state-owned banks. • Bank customers reported issues with online payments, banking apps, and, in very few cases, accessing ATMs. • These attacks were associated with fake SMS messages sent to Ukrainian phones to induce panic.
22 February–7 March 2022	• Phishing and DDoS attacks targeting Ukrainian entities in the public, military, and information sectors – FancyBear/APT28, Ghostwriter/UNC1151, Mustang Panda, or Temp.Hex.	• Exposure of information enabling the identification of individuals. • Restriction of access to information. • Destabilisation of civil infrastructure.
24 February 2022	• DDoS attack on the news website. • Malware attack. • 'IsaacWiper' on government entities. • Phishing campaign targeting the public sector delivering the 'SunSeed' malware.	• A DDoS attack paralysed The Kyiv Post's systems, forcing them to find alternative ways of publishing news by posting shortened articles on Facebook, Twitter, and LinkedIn. There were logistical issues related to the non-functioning personnel system and significantly more challenging communication between employees. • ESET, s.r.o., identified another cleansing element in Ukrainian government's networks that affects organisations not targeted by HermeticWiper and has no similarity in code. On 25 February 2022, the attackers released a new version of IsaacWiper with debugging logs, indicating that the attackers were unable to wipe some of the compromised computers.
2 February 2022	• Cyberattack on a border control checkpoint. • Websites of Ukrainian universities targeted – Brazil Threat Actor Group – theMx0nday. • Attack on a satellite Internet service.	• At a Ukrainian border control post, a cyberattack occurred involving data deletion, slowing down the process of allowing refugees to enter Romania. • 25 February 2022 – Attacked websites of Ukrainian. universities – Brazil Threat Actor Group – theMx0nday. • Cyber incident – an attack on the satellite Internet service Viasat caused a partial network outage for customers in Ukraine and beyond in Europe who rely on its KA-SAT satellite.

(*continues*)

Table 1. Continued.

Date	Type of threat	Consequences
28 February 2022	• Attacks by the Trojan 'Foxblade' (aka HermeticWiper) on public/private sector and military. Microsoft has detected a new series of offensive and destructive cyberattacks targeting Ukraine's digital infrastructure. These include attacks on the financial sector, agriculture, crisis response services, humanitarian aid as well as organisations and enterprises in the energy sector.	• Difficulties in civilian access to finances, food, and energy sources. • Destabilisation of civil infrastructure. • Disinformation. • Attempted theft of information enabling the identification of individuals associated with health, insurance, and transportation as well as other sets of government data.
4 March 2022	• Malware attacks on non-governmental organisations.	• Malicious software was specifically targeted at charitable organisations, non-governmental organisations, and other aid organisations to spread confusion and cause disruptions. • The aim of the attack was to disrupt the delivery of medicines, food, and clothing during the armed conflict.
29 March 2022	• Cyberattack on the IT infrastructure of Ukrtelecom.	• Hacker attack on Ukrainian websites. Because of the breach, some internal systems were reset, leading to the loss of access for certain local subscribers.
12 July 2023	• Malware attacks on diplomats in Kyiv.	• The hackers targeted at least 22 out of approximately 80 foreign missions in Kiev. Hackers from the group known as APT29 or 'Cozy Bear' intercepted and copied a car sale offer from one of the Polish diplomats. Subsequently, they embedded malicious software in it and sent it to dozens of other diplomats stationed in Kiev.

Sources:
https://stinet.pl/ukraina-historia-cyberatakow-cz-1-2/. [Accessed: Dec. 30, 2023];
https://www.gazetaprawna.pl/wiadomosci/swiat/artykuly/8333044,ukraina-hakerzy-atak-strony-rzadowe.html. [Accessed: Dec. 30, 2023];
https://www.money.pl/gospodarka/cyberatak-hakerow-na-ambasady-w-kijowie-wykorzystali-oferte-sprzedazy-samochodu-6918742318898016a.html. [Accessed: Dec. 30, 2023];
https://www.pap.pl/aktualnosci/news%2C1089376%2Czmasowany-atak-hakerski-na-ukrainie-nie-dzialaja-strony-wielu-organow. [Accessed: Dec. 30, 2023].

Among the cyberattacks on Ukraine, actions with a sabotage character have been documented. These attacks were carried out to disrupt the normal functioning of critical infrastructure systems, such as power plants, energy systems, or telecommunications. Cyberattacks have intensified significantly since Russia declared war on Ukraine. The DDoS attack from February 2022 is considered the largest to date in Ukraine. Many Ukrainian websites, such as those of banks, government, and the military, were inaccessible.

Temporarily, the websites recovered within a few hours. Such actions indicate an intention to instigate panic. This type of attack is aimed at disorganising the military, disrupting communication, and manipulating information.

3.2. The impact of cyberattacks on the volatility of the WIG_UKRAIN index

Some attacks aimed at disrupting the normal functioning of the government, creating chaos in society, or undermining trust in public institutions. The consequences of such actions involve not only manipulating information but also influencing public opinion at home and abroad.

It is worth emphasising that the motives behind attacks on Ukraine were complex and involved a combination of different objectives. Moreover, the scale and type of attacks change depending on the developments on international stage.

Figure 1 depicts the performance of the WIG_UKRAIN and WIG indices. Selected cyberattacks are marked with red arrows. The trends in which both indices were examined are generally in agreement. The correlation coefficient for the levels of quotations in the examined period is 0.3369. Its not very high value is primarily influenced by the period after Russia's aggression on Ukraine when initially both indices lost value. However, since the end of 2022, the WIG index entered a strong upward phase, while the WIG_UKRAIN index continues to lose value. It is challenging to expect an increase in the value of the index of Ukrainian companies operating in such difficult times under uncertain political and economic conditions.

Table 2 presents return rate statistics during the period of a cyberattack and the period following the cyberattack. Throughout the entire period, the WIG_UKRAIN index experienced an average decrease of 0.0020% per session, while the WIG index saw an average increase of 0.0309% per session. The provided statistics allow for the distinction of two sub-periods, that is, until 2022 and from 2022 onwards. Before 2022, the changes were not as significant as they were after 2022. Generally, the commencement of military actions in 2022 significantly increased the volatility of WIG_UKRAIN index quotations, which is an expected situation, as markets tend to react poorly to uncertainty.

Cyberattacks in Ukraine until 2022 did not inflict significant damage on the value of the index of Ukrainian companies. The attack

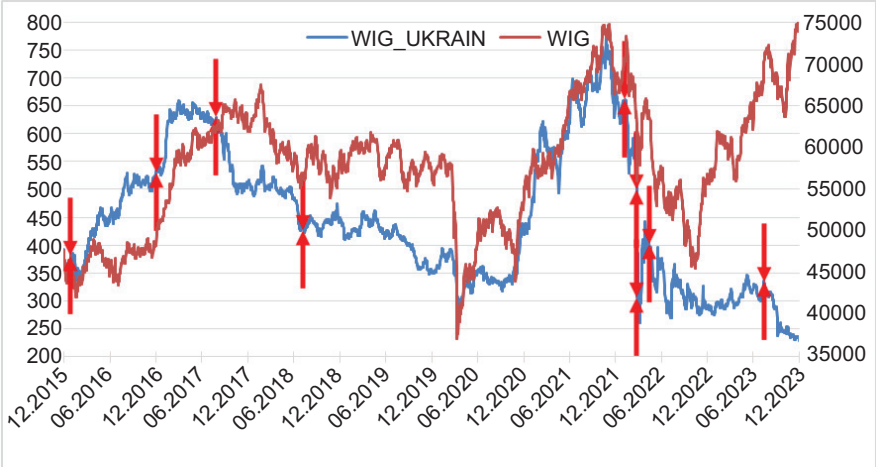

Figure 1. Performance of the WIG_UKRAIN and WIG indices from December 2015 to December 2023. *Explanations*: left axis – WIG_UKRAIN; right axis – WIG.
Source: Own compilation based on Warsaw Stock Exchange (GPW) data.

Table 2. Return rate statistics.

Cyberattacks	WIG_ UKRAIN			WIG		
	Mean –0.0020%			Mean 0.0309%		
	Day	Next day	5-Day mean	Day	Next day	5-Day mean
23 December 2015	0.66%	0.68%	0.96%	0.31%	0.00%	–0.46%
17 December 2016	–1.37%	0.19%	–0.53%	0.03%	0.70%	0.07%
23 December 2016	–0.25%	0.69%	0.38%	–0.25%	0.14%	0.13%
28 December 2016	1.06%	–0.07%	0.66%	–0.08%	0.73%	0.45%
27 July 2017	0.72%	0.85%	–0.08%	–0.31%	0.31%	0.02%
11 July 2018	0.07%	–0.17%	–0.03%	–0.87%	0.23%	–0.20%
13 January 2022	0.41%	–2.41%	–1.93%	–0.12%	–0.93%	–0.72%
14 & 15 January 2022	–2.41%	–1.93%	–1.99%	–0.93%	–0.43%	–0.92%
15–28 February 2022		–2.39%			–0.67%	
4 March 2022	–6.97%	–12.28%	–1.20%	–4.30%	0.30%	–0.37%
29 March 2022	15.80%	–5.31%	2.35%	1.58%	0.47%	0.35%
12 July 2023	–0.04%	0.86%	0.52%	2.55%	0.10%	1.00%

on the energy sector conducted on 17 December 2016 caused maximum damage to the index. In this case, the statistics of the WIG_UKRAIN index compared to WIG look significantly worse. Any other highlighted cyberattack in the period until 2022 did not result in a permanent loss of value for the WIG_UKRAIN index, compared

to WIG. One could even say that the market did not react to such cyberattacks. Moreover, even the attack on 27 July 2017, which was considered the largest in history at that time, remained practically unnoticed by the stock exchange.

The situation changed from 2022 onwards. With the onset of military actions, the stock market became significantly more sensitive to any information coming from Ukraine. The average change in the value of the WIG_UKRAIN index from February 2022 to the end of 2023 was -0.1195% per session. Meanwhile, during periods of intensified cyberattacks, especially the day after an attack, return rates reached significantly lower values. Only the attack on 12 July 2023 had a minor impact, but it was an attack without significant economic importance. However, every attack with potentially severe economic consequences from 2022 contributed to decline in the value of Ukrainian-listed companies

4. Conclusions

The global geopolitical situation plays a significant role in shaping global financial markets. Financial market sensitivity refers to the ability to respond to various factors, such as changes in the economy, political events, volatility in commodity prices, or factors disrupting the sense of security in a country. Rise in international tensions, conflicts, international negotiations, and political changes particularly impact the sensitivity of the stock market. The geopolitical situation in Ukraine has exposed entities operating in the capital market to increased cyberattack risks. However, companies are increasingly aware of the importance of investing in cybersecurity measures to protect their operations, data, and reputation. Ukrainian-listed companies must maintain a proactive approach to cybersecurity, continually adapting to new threats and changing regulations. Collaboration with governmental and international entities, comprehensive employee training, and the implementation of advanced cybersecurity technologies are crucial in the current efforts to protect Ukraine's economic well-being in the digital age.

A review of selected cyberattacks on Ukraine, characterised as sabotage, indicates that the primary targets were critical infrastructure, such as power plants, energy systems, and telecommunications. The intensity of these attacks has increased since Russia declared war on Ukraine. The attacks had complex motives, such as disrupting government operations, creating social chaos, and undermining trust in public institutions. The goals also involved disrupting

the armed forces, interfering with communication, and manipulating information.

Disruptive cyberattacks have resulted in the hindrance of telecommunications and the Internet services, restricted access to financial resources, and disrupted flow of news, and historically, they have been demonstrated to cause the denial of access to essential utilities, such as electricity, heating, and water. For instance, an incident on 29 March 2022 targeted Ukrtelecom, resulting in a connectivity collapse to only 13% of pre-war levels, causing nationwide disruption. The dissemination of false information and propaganda, often executed through attacks on the media sector, has a destabilising impact by influencing the information landscape and limiting the public's access to timely, trustworthy, and official information. This erosion of reliable information undermines trust in institutions through the manipulation of information. Furthermore, the compromise of data, including hacking and leaks facilitated by hacktivist groups, has led to the widespread publication of substantial volumes of organisational and individual data online, with potential unknown long-term consequences.

Cyberattacks not only led to information manipulation but also influenced public opinion both domestically and internationally. They stirred uncertainty, weakened trust in institutions, and affected societal stability.

An analysis of stock indices (WIG_UKRAIN and WIG) suggests that the market became more sensitive to information related to attacks from 2022 onwards, especially after Russia's aggression against Ukraine. Before 2022, cyberattacks on Ukraine had no significant impact on the value of Ukrainian company indices, except for the attack on the energy sector in December 2016. The situation changed from 2022 onwards, where every potentially economically harmful attack contributed to the decline in the value of Ukrainian-listed companies. With the onset of military actions, the stock market reacted more dynamically to cyberattacks. The returns of Ukrainian-listed companies reached lower values in the days following attacks, indicating increased market sensitivity to events related to the conflict.

Based on the conducted analyses, it is concluded that cyberattacks on Ukraine had a significant impact not only on infrastructure but also on financial markets and public opinion, especially after the start of military actions. The observed dependency confirms the growing sensitivity of the stock market to events related to

cybersecurity. The Ukrainian government is taking steps to secure against cyber threats; however, education, international collaboration, and regular system updates remain crucial in combating such attacks.

It is important to underscore the importance of the effectiveness of cyber defence by Ukraine in repelling attacks and/or mitigating their impact [23]. Ukraine bolstered the resilience of its national ICT infrastructure and cyber incident response prior to and during the war, in cooperation with allied governments and private companies [24]. Ukraine's private sector has also largely contributed to this process [25]. This included activities to strengthen the cyber resilience of Ukraine prior to and since the 2014 and 2022 military invasions, and cooperation with the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) [26]. Ukraine's preparation, recognising that it has been the subject of cyberattacks for many years, has involved private–public partnerships. With the outbreak of the war, private actors, such as Microsoft, Google, Amazon, and ESET, s.r.o., have publicly acknowledged the role played in terms of tracking and forecasting cyber threats [27], hosting of governmental data in the public cloud outside Ukraine, and other forms of collaboration by the Government of Ukraine to thwart cyber threats [28–31].

References

[1] T. Johansmeyer. (2022). *The cyber insurance market needs more money.* Harvard Business Review. [Online]. Available: https://hbr.org/2022/03/the-cyber-insurance-market-needs-more-money. [Accessed: Dec. 27, 2023].

[2] H. Korzeniowska, *Edukacja dla bezpieczeństwa w systemie oświatowym Europy na przykładzie Polski i Słowacji*. Cracow: EAS, 2004.

[3] K. Chałubińska-Jentkiewicz, "Cyberbezpieczeństwo – Zagadnienia definicyjne," *Cybersecurity and Law*, vol. 2, no. 2, pp. 7–23, 2019, doi: 10.35467/cal/133828.

[4] J. Wasielewski, "Zarys definicyjny cyberprzestrzeni," *Przegląd Bezpieczeństwa Wewnętrznego*, vol. 5, no. 5, pp. 225–234, 2013.

[5] J. Kisielnicki, *Systemy informatyczne zarządzania*. Warsaw: Placet, 2009.

[6] P. Sienkiewicz, "Terroryzm w cybernetycznej przestrzeni," in *Cyberterroryzm – nowe wyzwania XXI wieku*, T. Jemioło, J. Kisielnicki, K. Rajchel, Eds., Warsaw: Wyższa Szkoła Informatyki, Zarządzania i Administracji, 2009.

[7] A. Karmańska, M. Łada, "Ujawnianie obszarów i czynników ryzyka w sprawozdaniach z działalności spółek giełdowych – Obserwacje wobec zmian regulacji prawnych," *Zeszyty Teoretyczne Rachunkowości*, vol. 103, no. 159, pp. 42–43, 2019, doi: 10.5604/01.3001.0013.3074.

[8] M. Bochenek, "Ryzyko i niepewność w naukach ekonomicznych – Rozważania semantyczne," *Ekonomia (Economics)*, vol. 21, no. 4, pp. 46–63, 2012.

[9] N. Iwaszczuk, *Ryzyko w działalności gospodarczej: Definicje, klasyfikacje, zarządzanie*. Cracow: IGSMiE PAN, 2021.

[10] K. Marcinek, *Ryzyko projektów inwestycyjnych.* Katowice: University of Economics in Katowice, 2001.

[11] C.L. Pritchanel, *Zarządzanie ryzykiem w projektach*. Warsaw: WIG-Press, 2002.

[12] E. Haapamäki, J. Sihvonen, "Cybersecurity in accounting research," *Managerial Auditing Journal*, vol. 34, no. 7, pp. 808−834, 2019, doi: 10.1108/MAJ-09-2018-2004.

[13] A. Refsdal, B. Solhaug, K. Stølen, *Cyber-risk management*. Series: Springer Briefs in Computer Science, Springer Cham, 2015.

[14] NetDilgence. (2014). *Netdiligence cyber claims study 2014*, Technical report, NetDilligence. [Online]. Available: https://netdiligence.com/. [Accessed: Dec. 29, 2023].

[15] D. Štrucl, "Russian aggression on Ukraine: Cyber operations and the influence of cyberspace on modern warfare," *Contemporary Military Challenges*, vol. 24, no. 2, pp. 103–123, 2022. doi: 10.33179/BSV.99.SVI.11.CMC.24.2.6.

[16] D. Svyrydenko, W. Możgin, "Hacktivism of the anonymous group as a fighting tool in the context of Russia's war against Ukraine," *Future Human Image*, vol. 17, pp. 39–46, 2022. doi: 10.29202/fhi/17/6.

[17] M.C. Arcuri, M. Brogi, G. Gandolfi, "The effect of cyberattacks on stock returns," *Corporate Ownership & Control*, vol. 15, no. 2, pp. 70–83, 2018, doi: 10.22495/cocv15i2art6.

[18] R. Jamilov, H. Rey, A. Tahoun. (Jun. 03, 2021). *The anatomy of cyber risk.* Working paper 28906, National Bureau of Economic Research, Cambridge. [Online]. Available: http://www.nber.org/papers/w28906. [Accessed: Dec. 27, 2023].

[19] M. Xu, Y. Zhang, "Data breach CAT bonds: Modeling and pricing," *North American Actuarial Journal*, vol. 25, no. 4, pp. 543–561, 2021. doi: 10.1080/10920277.2021.1886948.

[20] M.C. Arcuri, L. Gai, F. Ielasi, E. Ventisette, "Cyber attacks on hospitality sector: Stock market reaction," *Journal of Hospitality and Tourism Technology*, vol. 11, no. 2, pp. 277–290, 2020, doi: 10.1108/JHTT-05-2019-0080.

[21] S. Tweneboah-Kodua, F. Atsu, W. Buchanan, "Impact of cyberattacks on stock performance: A comparative study," *Information and Computer Security*, vol. 26, no. 5, pp. 637–652, 2018, doi: 10.1108/ICS-05-2018-0060.

[22] K.T. Smith, L.M. Smith, M. Burger, E.S. Boyle, "Cyber terrorism cases and stock market valuation effects," *Information and Computer Security*, vol. 31, no. 4, pp. 385–403, 2023, doi: 10.1108/ICS-09-2022-0147.

[23] Microsoft. (Jun. 22, 2022). *Defending Ukraine*: *Early lessons from the cyber war*. [Online]. Available: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE50KOK. [Accessed: Feb. 20, 2024].

[24] S. Landau. (Sep. 30, 2022). *Cyberwar in Ukraine*: *What you see is not what's really there.* Lawfare. [Online]. Available: https://www.lawfareblog.com/

cyberwar-ukraine-what-you-see-not-whats-really-there. [Accessed: Feb. 20, 2024].

[25] E. Schroeder, S. Dack. (Feb. 27, 2023). *A parallel terrain*: *Public-private defense of the Ukrainian information environment*. [Online]. Available: https://www.atlanticcouncil.org/in-depth-research-reports/report/a-parallel-terrain-public-privatedefense-of-the-ukrainian-information-environment/. [Accessed: Feb. 20, 2024].

[26] State Service of Special Communications and Information Protection of Ukraine. (Jan. 19, 2023). *Ukraine has signed an agreement on accession to the NATO.* Cooperative Cyber Defence Centre of Excellence. [Online]. Available: https://cip.gov.ua/en/news/ukrayina-pidpisala-ugodu-pro-priyednannya-do-ob-yednanogo-centru-peredovikh-tekhnologii-zkiberoboroni-nato. [Accessed: Feb. 20, 2024].

[27] Microsoft. (Jun. 22, 2022). *Defending Ukraine*: *Early lessons from the cyber war*. [Online]. Available: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE50KOK. [Accessed: Feb. 20, 2024].

[28] G. Corfield. (Jan. 7, 2023). *Russian cyberattacks on Ukraine halved with help from Amazon and Microsoft.* [Online]. Available at: https://www.telegraph.co.uk/business/2023/01/07/russian-cyberattacks-ukraine-halved-help-amazon-microsoft/. [Accessed: Feb. 20, 2024].

[29] S. Pell. (Dec. 1, 2022). *Private-sector cyber defense in armed conflict.* [Online]. Available: https://www.lawfareblog.com/private-sector-cyber-defense-armed-conflict. [Accessed: Feb. 20, 2024].

[30] I. Sánchez Cózar, J.I. Torreblanca. (Mar 7, 2023). *Ukraine one year on*: *When tech companies go to war*, European Council on Foreign Relations. [Online]. Available: https://ecfr.eu/article/ukraine-one-year-on-when-tech-companies-go-to-war/. [Accessed: Feb. 20, 2024].

[31] J. McLaughlin. (Mar. 3, 2023). *Russia bombards Ukraine with cyberattacks, but the impact appears limited*. [Online]. Available: https://www.npr.org/2023/02/23/1159039051/russia-bombards-ukraine-with-cyberattacks-but-the-impact-appears-limited. [Accessed: Feb. 20, 2024].