ACIG
APPLIED CYBERSECURITY & INTERNET GOVERNANCE

NASK

Investment in Cybersecurity Companies in Times of Political and Economic Instability

Grzegorz Przekota | Koszalin University of Technology, Poland | ORCID: 0000-0002-9173-2658

Abstract

The socio-economic development that has taken place in recent years takes into account cybersecurity issues. Cybersecurity has many different dimensions, including the economic dimension. The Russian-Ukrainian conflict has shown that modern war is not only conventional, but also cybernetic. Earlier, the massive shift to remote communication systems forced by COVID also increased the demand for cybersecurity. This means that cybersecurity companies receive new orders, which can have a positive impact on their financial results. In the opinion of many experts, investing in such companies could be a good business. The research conducted in this article focuses on testing assumptions related to the recognition of investments in technology companies as prospective investments. Therefore, this study examines the impact of Russia-Ukraine war (from February 2022 to December 2024) and the COVID pandemic (from March 2020 to February 2022) on the valuation of cybersecurity companies. The period from January 2015 to February 2020 was used as the comparative period. The research material consists of companies and stock indices from the American and Polish markets. The results of the research are inconclusive. In fact, there are some examples of companies that took advantage of the Russian-Ukrainian conflict to achieve above-average returns. Such a business is risky, which is why these companies are achieving above-average returns with increased shares price volatility. However, it turns out that automatically assigning a company to the

Received: 18.03.2024

Accepted: 01.06.2024

Published: 18.07.2024

Cite this article as:
G. Przekota "Investment in cybersecurity companies in times of political and economic instability," ACIG, vol. 3, no. 1, 2024, DOI: 10.60097/ACIG/190342

Corresponding author:
Grzegorz Przekota, Koszalin University of Technology, Poland.
E-mail: grzegorz.przekota@tu.koszalin.pl;
0000-0002-9173-2658

cyber or IT category does not mean that it will be a good investment in times of war or pandemic.

Keywords

cybersecurity threat, enterprise development, investments, stock exchange

1. Introduction

In recent years, the importance of concepts such as the computerisation of the economy, modern technologies, the Internet of things, information security, and cybersecurity has been particularly emphasised [1]. They are related to modern production processes that are increasingly computerised, in the provision of both material goods and services.

The last few years in the Eastern European region have been years of anxiety related to the Russian-Ukrainian conflict. This is an event that directly or indirectly has affected all European countries and a significant number of non-European countries. The war has affected the world not only in the physical dimension but also in the cyberspace dimension. Modern conflicts are not only conducted in a conventional way but also in a hybrid way, and the parties to the conflict make extensive use of the cyber world. Governments, companies, and individuals are being attacked through information technology (IT) networks. Cyberattacks have prompted decision-makers and companies to take active steps to limit the impact of cyberattacks. On the one hand, society is being made aware of media manipulation, which is most easily carried out via Internet media, and on the other hand, systems and software are being built to protect against cyberattacks. This is where business issues come into play. On the one hand, war results in significant human and material losses, on the other hand, it is a profitable industry for both arms and IT sectors.

External threats that negatively impact cybersecurity have quickly become an extreme risk and threat to global development [2]. Addressing this challenge from a global perspective requires appropriate and focused resolve [3].

Cybersecurity is associated with technical security measures and solutions, such as encryption, intrusion prevention systems, and access control to IT systems. The business aspects of cybersecurity have been growing for at least 40 years [4]. In his reflections at the time, Courtney stated that the decision whether to protect against

IT attacks requires weighing all the costs and benefits, and that security controls should not be implemented if they cost more than tolerating the problem. This approach is related to the neoclassical approach to economic problems, which is dominated by rationality and optimisation of behaviour [5]. Reality, however, is more stochastic and uncertain, and information is not perfect.

A World Economic Forum report identified cybersecurity failures as a clear and present threat. The scale of cybersecurity threat is difficult to estimate [6]. Different sources come up with different calculations. According to data, by 2020, the cost of cybercrime was estimated at $1 trillion and investments in cybersecurity stood at $145 billion [7], with these values growing rapidly from year to year [8]. The difficulty in estimating the cost of cybercrime is primarily due to the complexity of the problem, while economic models simplify reality. Therefore, all research that addresses the issue of cybercrime and cybersecurity develops the perception of the problem and shows the extent of its impact, both direct and indirect.

Cybersecurity is a very broad concept. It is defined differently in the literature on the subject. From the point of view of this study, it can be assumed that cybersecurity includes various procedures that create a secure environment by protecting assets, and an asset is anything that has a certain value [9]. Assets are those things that require special protection against illegal access, use, disclosure, modification, destruction, and/or theft that could result in loss to the organisation. Because assets are of different types, the scope of cybercrime is very broad, ranging from the theft of data or the disclosure of confidential or compromising information to attacks on physical assets.

A broad economic view of cybersecurity is proposed by Rathod and Hämäläinen, who formulate public policy recommendations aimed at adapting policies and regulations to ensure trust in the digital environment, and also postulate a combination of economic and cybersecurity analysis that provides reference points for the economic assessment of national and international cybersecurity audits and standards [10]. Meanwhile, Ahmed notes that cybercrime costs companies and countries significant amounts of money and disrupts economic and financial activities around the world [11]. Estimates of the financial and physical costs associated with cybercrime motivate investment in cybersecurity. While it is the responsibility of governments to ensure that laws are in place to combat cybercrime, all organisations need to take protective measures commensurate with the threat. This is where companies

that develop and supply software to protect organisations' assets come into play. This is undoubtedly a developing industry. For example, in Poland, the participation of Section J (Information and Communication) in gross domestic product (GDP), which includes Section 62 – Activities related to software and IT consultancy and related activities – was at a record high of 4.92% of GDP in 2022, increasing by more than 1 percentage point over the last decade [12].

There are reports and publications on news websites and specialised websites that suggest that investing in cybersecurity companies is currently one of the best forms of investing capital (see, Websites). Such studies are an important part of financial markets because they influence investor's opinion.

Organisations defend themselves against cyber threats in a variety of ways. There is some debate in the literature about how the level of security depends on the design of the system, whether the defence depends on the efforts of the laziest defender, the bravest defender, or the sum of all defenders [13]. Basically, it corrects the idea that a software company should hire fewer but better programmers, more testers, and the best security architect it can find [14]. From the point of view of investors in a company's shares, it is extremely difficult to assess, but this can be done indirectly by assessing the market success of the software that the company sells.

Based on the suggestion that investing in cybersecurity companies is a profitable business, following are the three objectives for this study:

1. To test whether software companies, especially those that provide protection against cyber threats, perform better than stock market indices that reflect the overall market situation.
2. To check whether the situation regarding investments in cyber companies in Poland, which is nearer to the Russian-Ukrainian conflict, is different from that in the United States.
3. To examine the impact of the war, compared to the impact of the COVID pandemic.

These are three issues that helped to test the recommendations for investing in technology companies.

2. Methods

The research focused on the rates of return for four American and four Polish companies. The choice of companies

was deliberate. In the case of the American companies, they are the largest cybersecurity companies listed on the NASDAQ stock exchange, including the following:

1. Cisco Systems (CSCO.US)
2. Palo Alto Networks Inc (PANW.US)
3. Fortinet (FTNT.US)
4. Check Point Software Technologies Ltd (CHKP.US)

These companies were evaluated against the NASDAQ index.

In the case of the Polish Stock Exchange, these companies are involved in the development and supply of software. The condition for participation in the study was that the company had been operating as a listed company for at least 9 years, including the following:

1. Asseco Poland SA (ACP)
2. Comarch SA (CMR)
3. Sygnity SA (SGN)
4. LSI Software SA (LSI)

These companies were evaluated against the Warsaw Stock Exchange General (WIG) index.

The period of the research covers the years 2015–2023 and is divided into the following three sub-periods:

1. January 2015–February 2020
2. March 2020–February 2022
3. February 2022–December 2023

Weekly frequency data was examined.

The division of periods coincided with the COVID pandemic and beginning of Russia's military operations in Ukraine, and the interest lies in determining the difference in the statistics of the companies' quotations against the relevant stock market indices during pandemic and after the start of hostilities, compared to the previous period.

The research is divided into two stages:

1. Price formation of share stock in relation to stock market indices. The data is presented in logarithmic form. This method

makes it easy to assess the rate of increase in the value of the quotations, as small differences can be seen:

$$\ln y_{t+1} - \ln y_t = \ln \frac{y_t + 1}{y_t} \approx \frac{y_{t+1}}{y_t} = -1$$

The graph uses a main unit of 0.5, which represents an increase in the value of the quotes of approximately 65%, regardless of the level. Separate graphs show the relative increases in price. These graphs show the strength of the changes and highlight periods of above-average change.

2. Overview of the descriptive statistics of the return rate series:
   - Mean – average of weekly returns interpreted as average weekly income;
   - St. Dev. – standard deviation of weekly returns, allowing the assessment of the absolute strength of diversification of returns, interpreted as total risk.

The research is supplemented by graphical representation of the company's return and risk on a risk-return graph in three time intervals.

3. Results

Figure 1 shows the share prices of the US-listed companies against the backdrop of the NASDAQ index. The NASDAQ index was in an upward trend until the end of 2021. However, from the beginning of 2022, it entered a short downward phase that lasted for 1 year. In 2023, the NASDAQ index began to recover, but the growth rate was quite slow and 2023 ended at a lower level than the 2021 peak.

The American market is a very large market and the companies listed there tend to be global companies. Therefore, the start of military operations in Ukraine may have caused some pessimism among investors about the possibility of further positive developments. This uncertainty was reflected in index declines in 2022. What experts often emphasise is that societies have become accustomed to certain situations, including tragic ones. This habit and the adaptation of companies to the new situation led to this negative trend being replaced by a moderately positive trend from 2023.

Interesting is how the cybersecurity companies, for whom the threat of cyberattacks is the basis for building commercial strategies and protection against cyberattacks is the main source of revenue,

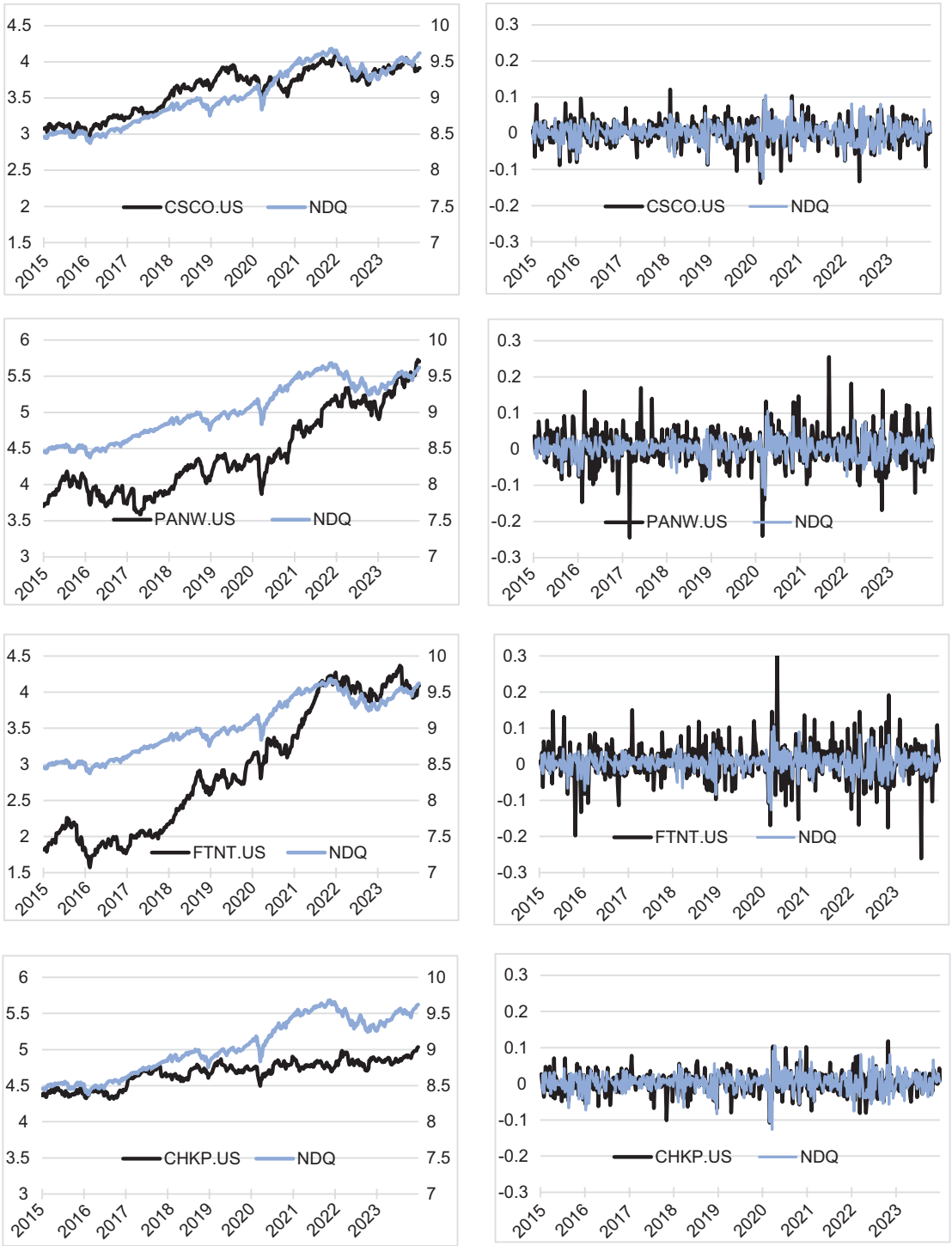

Figure 1. Share price performance of the US technology companies, 2015–2023.

have coped with this situation. It turns out that, in general, all the companies recorded an increase in value throughout the period, but the pace of this increase varied, with the highest being PANW and FTNT, and the clearly weaker being CSCO and CHKP. PANW and FTNT grew at a rate well above that of the NASDAQ index, the third at a similar rate to the NASDAQ and the last at a much slower rate. Therefore, the mere qualification as a modern technology company was not enough to achieve a good growth rate, which proves the rationality of investors who make decisions based on other information as well. It should be noted that all four companies are being promoted in the media as potentially good investments.

The COVID pandemic did not stop this growing trend, but rather strengthened it. The disruption was only temporary at the beginning of the pandemic announcement, but the short-term declines were significant; then there were increases.

What happened after the outbreak of hostilities in Ukraine is particularly interesting. In the period following the outbreak of war, PANW was the best performer, with a spectacular increase in value. The company is constantly monitoring the situation regarding cyberattacks related to the Russian-Ukrainian war [15].

The graphs on the right side show the rates of return. The most interesting concern is the volatility following Russia's invasion of Ukraine. There is a slightly larger increase in volatility. However, even in the period up to 2022, there are sub-periods with increased volatility, such as the pandemic period. In general, it is natural for any period of economic or political uncertainty to increase volatility in capital markets.

The situation on the Polish stock market was different (Figure 2). First, until the end of 2021, the WIG index was in a very weak upward trend. The year 2022, similar to the NASDAQ, was a year of decline, but the year 2023 brought a strong recovery in value, and the WIG index saw the end of 2023 with a record value.

The COVID pandemic initially caused a significant drop, but then WIG prices started to rise. However, companies behaved differently.

It is worth noting that Polish companies do not have the same influence as American companies. In terms of capitalisation, the Polish companies analysed are clearly inferior to their American counterparts. The fourth American company analysed by capitalisation,

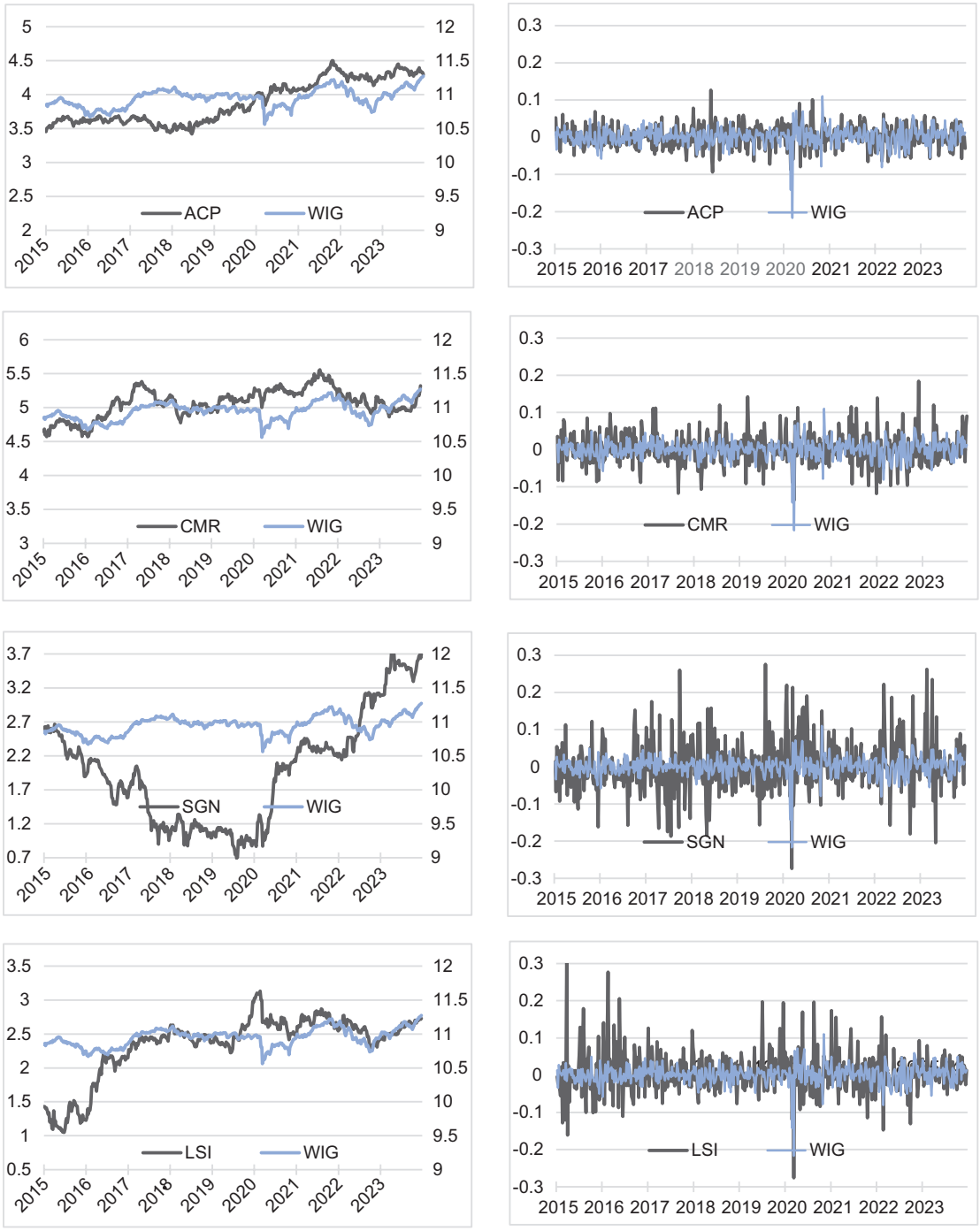

Figure 2. Share price performance of Polish technology companies, 2015–2023.

CHKP, has a capitalisation ten times higher than the largest Polish company analysed, ACP.

Taking into account the situation after Russia's aggression against Ukraine, the best Polish company is SGN, which intensively implements software in Ukraine as well.

The characteristics noted in the graphs are translated into rates of return descriptive statistics (Table 1). First of all, we observed that the range of average returns increases in the pandemic period and after Russia's invasion of Ukraine:

- For the American market:
  - Until March 2020 – the range was between 0.18% for CHKP and 0.59% for FTNT.
  - Between March 2020 and February 2022 – the range was between 0.17% for CHKP and 1.14% for FTNT.
  - From February 2022 – the range was between -0.05% for CSCO and 0.82% for PANW.
- For the Polish market:
  - Until March 2020 – the range was between -0.25% for SGN and 0.80% for LSI.
  - Between March 2020 and February 2022 – the range was between -0.13% for LSI and 1.17% for SGN.
  - From February 2022 – the range was between 0.03% for LSI and 1.75% for SGN.

Table 1. Descriptive statistics of time series of weekly returns.

Index/ company	01.2015–03.2020		03.2020–02.2022		02.2022–12.2023	
	Mean (%)	St. Dev.	Mean (%)	St. Dev.	Mean (%)	St. Dev.
NDQ	0.29	2.13	0.40	3.50	0.16	3.27
CSCO.US	0.30	3.11	0.33	3.68	-0.05	3.42
PANW.US	0.36	4.52	0.83	5.89	0.82	5.83
FTNT.US	0.59	4.37	1.14	6.33	0.19	6.41
CHKP.US	0.18	2.69	0.17	3.54	0.21	3.05
WIG	0.06	1.87	0.20	3.72	0.23	2.84
ACP	0.25	2.88	0.31	3.31	0.05	3.05
CMR	0.31	3.96	0.02	4.63	0.25	4.38
SGN	-0.25	6.80	1.17	6.87	1.75	7.59
LSI	0.80	5.80	-0.13	6.42	0.03	3.86

These results intend that the pandemic and the war have significantly widened the gap between companies' average weekly returns, compared to the previous period. Companies are therefore coping with political and economic instability in very different ways, with some being benefitted and others losing out.

For all US companies, the standard deviation increases after 2020 and 2022. Similarly for all Polish companies until 2020, and for three of the four Polish companies after 2022 (except LSI). The value of standard deviation for the whole stock market (standard deviation of the indices) also increases. Interestingly, however, the volatility measured by the standard deviation from February 2022 is lower for the Polish stock exchange, which is closer to the conflict, than for the American stock exchange.

In general, it would appear that modern IT companies achieve better financial results after the outbreak of hostilities and the increased number of cyberattacks, which is reflected in above-average increases in share prices. This assumption is also consistent with many of the articles cited above, which encourage investment in technology companies. However, the situation is more complicated. This is shown in Figure 3.

The COVID pandemic situation and the subsequent war in Ukraine have changed the stock market situation for cybersecurity companies. Every company behaves differently.

Taking into account the detailed objectives of the research, it can be said that technology companies in the period of economic and political stabilisation do not stand out from the stock market indices as companies with above-average returns. However, the economic destabilisation that took place during the COVID pandemic, or the political destabilisation that has taken place since the war in Ukraine, causes the results of the companies to become more uneven, with some performing better and others worse. The war and the pandemic have increased the overall volatility in both Poland and the United States. Capital markets are global markets, so stock market reactions are often similar, even if they are in different regions of the world.

Companies that have benefited from the COVID pandemic include FTNT and PANW in the United States and SGN in Poland. Of them, PANW from the United States and SGN from Poland increase in value during war. In general, the situation of PANW from the US market and SGN from the Polish market can be described as classic.

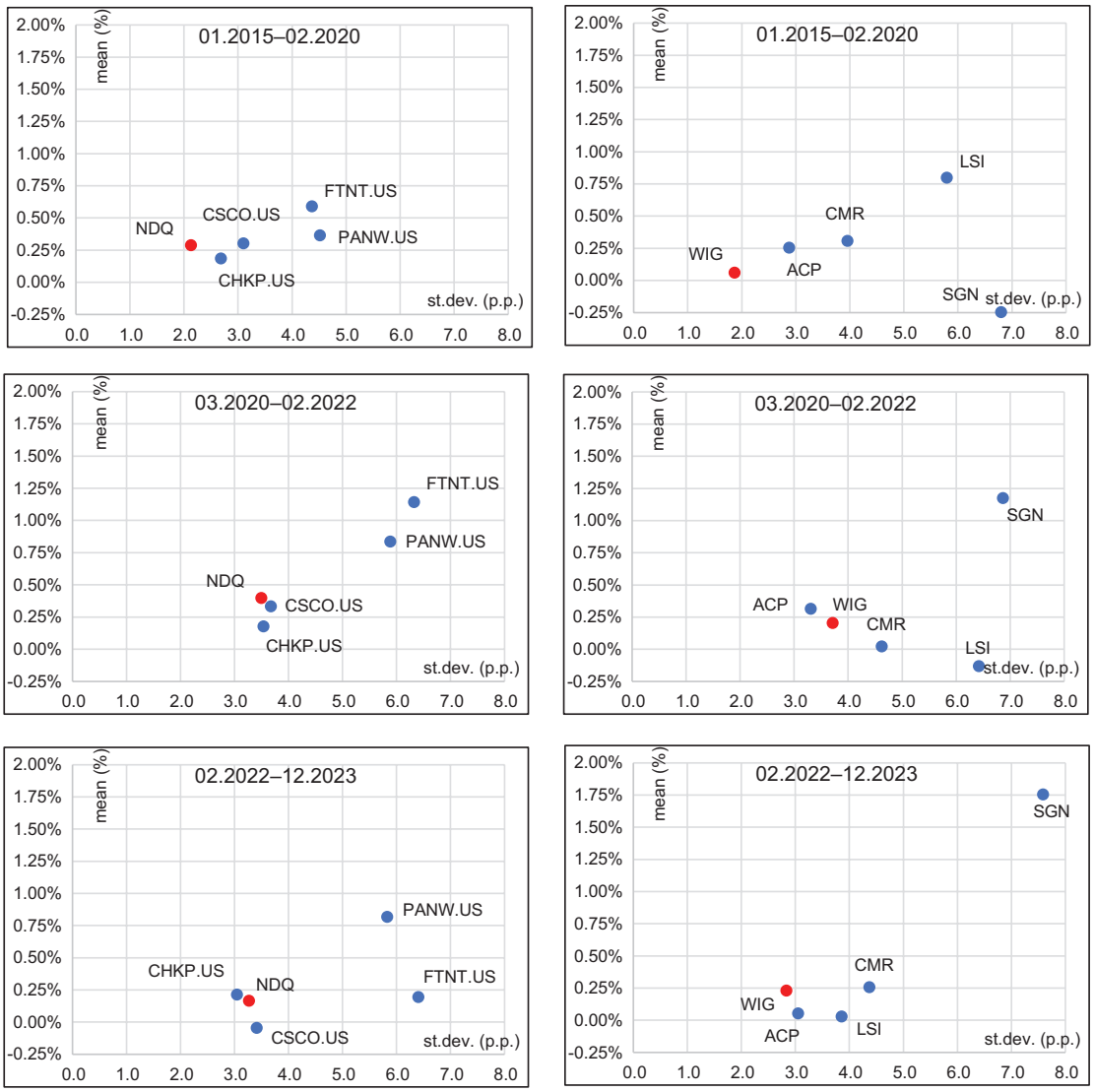

Figure 3. Risk-return map for technology companies in the United States and Poland.

On the charts, these companies are located in the upper right corner (03.2020–02.2022 and 02.2022–12.2023). The position of the risk-return map in the upper right corner of the chart means that such a company has achieved high returns with significant price volatility. This is a classic situation for companies involved in risky projects, such as cyber threats related to the Russian-Ukrainian conflict. The situation of other companies is very different. Some have lost their growth momentum after 2022, others have gained. Each company has its own specificities, and it is not possible here to generalise the same.

4. Conclusions

The war industry has always been seen as a harbinger of economic change. Countries that fought wars to gain a military advantage developed techniques and technologies. This development was later transferred to the production of civilian goods and services. Today's warfare has not only a classical dimension but also a cybernetic one. And, it is the cybernetic advantage that often gives rise to the conventional advantage. One of the manifestations of cyber warfare is cyberattacks and cyber threats. The cybernetics industry, both those used to attack and those used to defend against attacks, is one of the fastest growing industries today. As a result, articles appear in the specialised press, encouraging investors to take an interest in cyber and IT companies.

Modern warfare is certainly changing the perception of high-tech, IT, and cyber companies. The use of drones itself shows that IT is crucial in such a war. Another expressions of this interest are the events related to cyberattacks, remote shutdown of equipment, data theft, destabilisation of banking systems, attacks on government institutions, etc. Any company dealing with high technologies is considered crucial in such conditions, and its solutions are analysed and implemented by decision-makers. The decision-makers themselves try to support and promote the development of cybernetic solutions and thus cyber companies.

It is against this background that the effectiveness of the activities of high-tech companies should now be assessed. Not every solution proposed by such companies is accepted by decision-makers or the market. This makes running such a business potentially very profitable, but also very risky. The research conducted in this thesis clearly shows that the mere fact that a company belongs to a group of companies involved in IT, cybersecurity, or high technology does not guarantee a successful investment. This can be seen in both American and Polish markets. However, taking into account the importance of the Russian-Ukrainian war in the company's strategy and implementing business solutions that take into account the economic changes caused by the war can contribute to greater market success. Investors should therefore critically assess the company's development potential and make decisions on this basis, rather than relying solely on press reports about the company's potential.

References

[1] R. Von Solms, J. Van Niekerk, "From information security to cybersecurity," *Computers & Security*, vol. 38, pp. 97–102, 2013, doi: 10.1016/j.cose.2013.04.004.

[2] W. Raghupathi, S.J. Wu, V. Raghupathi, "The role of information and communication technologies in global sustainability: A review," *Journal of Management for Global Sustainability*, vol. 2, no. 1, pp. 123–145, 2014.

[3] K.L.-T. Low, C.S. Lim, A. Samudhram, "Sustainable economic development: A perspective from ICT loops in developing nations," *African Journal of Business Management*, vol. 5, no. 15, pp. 6138–6149, 2011, doi: 10.5897/AJBM10.529.

[4] R.H. Courtney Jr., "A systematic approach to data security," *Computers & Security*, vol. 1, pp. 99–112, 1982, doi: 10.1016/0167-4048(82)90003-7.

[5] P. Dixon, D. Jorgenson, *Handbook of Computable General Equilibrium Modeling*, Elsevier, North Holland, 2012.

[6] M. McLennan, *The global risks report*, 16th ed. Geneva: World Economic Forum, 2021.

[7] J. Lewis, Z. Smith, E. Lostri. (2020). *The hidden costs of cybercrime*. [Online]. Available: https://www.csis.org/analysis/hidden-costs-cybercrime. [Accessed: Aug. 17, 2021].

[8] Verizon, *Data Breach Investigations Report,* 2020. [Online]. Available: https://itb.dk/wp-content/uploads/2020/07/verizon-data-breach-investigations-report-2020.pdf. [Accessed: Aug. 17, 2021].

[9] International Organization for Standardization, *Information technology – Security techniques – Code of practice for information security controls (AS ISO/IEC 27002:2015)*, 2015. [Online]. Available: https://www.iso.org/standard/43757.html. [Accessed: Aug. 17, 2021].

[10] P. Rathod, T.A. Hämäläinen, "A novel model for cybersecurity economics and analysis." 17th IEEE International Conference on Computer and Information Technology, 2017, pp. 274–279, doi: 10.1109/CIT.2017.65.

[11] E.M. Ahmed, "Modelling information and communications technology cyber security externalities spillover effects on sustainable economic growth," *Journal of the Knowledge Economy*, vol. 2, pp. 1–19, 2020, doi: 10.1007/s13132-020-00627-3.

[12] Statistics Poland. (May 10, 2024). *Macroeconomic Indicators*. [Online]. Available: https://stat.gov.pl/wskazniki-makroekonomiczne. [Accessed: May 17, 2024].

[13] H. Varian, "System reliability and free riding," in *Economics of information security*, L.J. Camp, S. Lewis, Eds., Dordrecht: Kluwer, 2004, pp. 1–15.

[14] R. Anderson, T. Moore, "Information security: Where computer science, economics and psychology meet," *Philosophical Transactions of the Royal Society a Mathematical, Physical and Engineering Sciences*, vol. 367, pp. 2717–2727, 2009, doi: 10.1098/rsta.2009.0027.

[15] Palo Alto Networks. (May 04, 2024). *Protect Against Russia-Ukraine Cyber Activity*. [Online]. Available: https://www.paloaltonetworks.com/russia-ukraine-cyber-resources. [Accessed: May 17, 2024].

Websites

https://www.lynxbroker.pl/inwestowanie/gielda/akcje/analiza-akcji/cyberbezpieczenstwo-5-propozycji-akcji. [Accessed: Jan. 12, 2024].

https://pfrsa.pl/aktualnosci/polski-sektor-cyberbezpieczenstwa-poznaj-startupy-ktore-poprawiaja-bezpieczenstwo-w-sieci.html. [Accessed: Jan. 10, 2024].

https://dnarynkow.pl/sektor-cyberbezpieczenstwa-najciekawszy-temat-inwestycyjny-dekady. [Accessed: Jan. 07, 2024].

https://gpwatak.pl/inne/cyberbezpieczenstwo-trend-w-najblizszej-przyszlosci. [Accessed: Jan. 12, 2024].

https://www.parkiet.com/analizy-rynkowe/art19680311-ukryte-perelki-w-sektorze-it. [Accessed: Jan. 07, 2024].

https://www.investors.com/news/technology/cybersecurity-stocks. [Accessed: Jan. 12, 2024].

https://www.fool.com/investing/stock-market/market-sectors/information-technology/cybersecurity-stocks. [Accessed: Jan. 11, 2024].

https://www.kiplinger.com/investing/stocks/tech-stocks/602685/cybersecurity-stocks-to-lock-up-growth. [Accessed: Jan. 10, 2024].

https://www.nasdaq.com/articles/6-cybersecurity-stocks:-which-is-the-best-to-buy. [Accessed: Jan. 07, 2024].

https://admiralmarkets.com/education/articles/shares/cybersecurity-stocks. [Accessed: Jan. 12, 2024].