UNIVERSITY OF TARTU

Faculty of Social Sciences

School of Economics and Business Administration

Yaroslav Nedvyga

ABNORMAL RETURNS OF US CYBERSECURITY STOCKS DURING COVID-19 PANDEMIC AND RUSSO-UKRAINIAN CONFLICT

Bachelor Thesis

Supervisor: Junior lecturer Mark Kantšukov

Tartu 2024

I have written this Bachelor Thesis independently. Any ideas or data taken from other authors or other sources have been fully referenced.

Table of contents

Introduction

During the time of uncertainties, such as COVID-19 pandemic, Russo-Ukrainian conflict, or any other crisis, the stock market experiences high volatility, panics, and losses. On February 2020, the S&P500, NASDAQ composite, and the Dow Jones Industrial Average declined by 33.9%, 30.1% and 37.1% (Song et al., 2022).

On the other hand, against such events, there are sectors that have notably outperformed, with the stocks of public companies in these sectors delivering abnormal returns to investors. There is a rationale to entertain the notion that the cybersecurity sector can be reviewed as such a sector.

The reasons why the author assumes that the cybersecurity sector could bring abnormal returns during the COVID-19 pandemic, and Russo-Ukrainian conflict are high demand for cybersecurity services, comparative high financial performance of the cybersecurity companies, and new technological infrastructures. Security is vital, the companies always need to secure their users, and customers in order to deliver their products or services. The cybersecurity software is considered as key component rather than an operational element (Fernandez De Arroyabe et al., 2023).

The author chose stocks of US companies because the largest number of cybersecurity companies are mostly publicly traded in the US markets. In the European market or any other markets, there are far fewer public companies, but there are a lot of private companies that provide cybersecurity services. (Gao et al., 2020)

There are many studies on the topic of positive or negative returns during different times of uncertainty, which observe different sectors and find various results. During the COVID-19 pandemic, the stock market crashed in March 2020, and stocks of the companies in sectors such as energy, retail, software, and healthcare brought positive returns to investors. On the contrary, real estate, entertainment, and hospitality sectors earned negative returns. (Mazur et al., 2021)

The previous study can be supplemented by another one, which found that the global economic downturn in 2008 and the COVID-19 pandemic adversely impacted a multitude of industries. The worst-performing sectors were precious metals, natural gas, hotels, motels, aircraft, and restaurants during that time. However, the top-performing sectors were coal, candy, soda, agriculture, medications, and computer software. (Chen & Yeh, 2021)

The first empirical study that was made for the evaluation of the stock market returns after Russia invaded Ukraine found that the conflict was the key factor of dropping the different stock markets down (Boungou & Yatié, 2022).

The aim of the Bachelor thesis is to assess the abnormal returns of stocks of cybersecurity companies traded on the US markets after the first month of the COVID-19 pandemic and the Russo-Ukrainian conflict. Since, to the author`s best knowledge, the assessment of abnormal returns in the US cybersecurity companies during the shocks were not studied, the author would try to fill the research gap and explain the results.

The author formulated the following research tasks, in order to achieve the aim of the thesis:

- to provide an overview of a concept of abnormal returns,
- to identify different approaches to calculating the abnormal returns,
- to consider from theoretical perspective the effects of external shocks on the stock returns,
- to provide the results of previous studies on abnormal returns during COVID-19 pandemic and Russo-Ukrainian conflict,
- to collect and process the data for the study,
- to conduct the event study for US cybersecurity stock performance during COVID-19 and Russo-Ukrainian conflict,
- to analyze and discuss the results of the study.

This study can be interesting to investors, or fund managers, who want to earn more returns. After understanding the results of this study, the investors or portfolio managers will be able to make deeper diversification during times of instability or crisis.

The following thesis is divided into two main chapters: theoretical and empirical parts. In the first chapter, the author provides overview of concept of abnormal returns, provides the methods of abnormal returns measurement, defines the advantages and disadvantages of different approaches for calculating the abnormal returns, then the author concludes the impact of external shocks on the stock market and how specific sectors can benefit from these kinds of events. At the end of this chapter, the author analyzes empirical studies on abnormal returns in context of COVID-19 pandemic and Russo-Ukrainian conflict, and make the conclusion.

The next chapter is the empirical analysis. The author makes an event study in order to compare the two different events, and its consequences on the stock returns of the US

cybersecurity companies. The author finds similarities and the differences between those events and bring the conclusion. There will be the comparison between abnormal returns of cybersecurity companies with NASDAQ composite index returns. The author chose the NASDAQ composite index because this one mostly consists of technological companies and the cybersecurity sector is considered a highly technological one.

Nevertheless, there are possible limitations of this thesis because the list of the cybersecurity companies in this work touches some companies that provide not only the cybersecurity services, but also some technology for IT specialists. This is a common story in cybersecurity and technology sectors, where some companies are consolidators and they operate not only in the cybersecurity, but also in observability, data analysis or AI.

Keywords: abnormal returns, COVID-19, cybersecurity, Russo-Ukrainian conflict, stock performance.

1. Abnormal returns of stocks in the context of external shocks – theoretical considerations

1.1. The approaches for measurement of stocks abnormal returns

The abnormal returns refer to exceptionally high gains or losses that are produced by specific assets within particular timeframe (Barone, 2023). In finance, these abnormal returns are often used in order to measure the impact of some specific events, such as wars, pandemics, earnings dates, and the publications of macro reports (Liu et al., 2021). The main concept behind the calculation of abnormal returns is the isolation of a specific event. It is more convenient to isolate one event with one asset, or stock portfolio in order to assess the returns within some timeframe.

It should be mentioned that abnormal returns can be positive, or negative. The positive abnormal returns refer to the asset, which performed better than expected. On the contrary, the negative abnormal returns refer to the asset, which suggests the underperformance (Gyamfi-Yeboah et al., 2012). In addition to that, the abnormal returns can be achieved by chance because of some unexpected event (Watts, 1978).

Acknowledging the research by Aboody et al. (1999), who highlighted the caveat that past performance does not always predict future results, investors actively scrutinize abnormal returns as potential indicators of future asset performance. These returns, deviations from expected market behavior, offer valuable insights into market dynamics and potential opportunities for outperformance or underperformance.

Looking at specific instances where abnormal returns occur, investors gain nuanced understandings of underlying market inefficiencies and can tailor their investment strategies accordingly. Whether abnormal returns consistently exceed or fall short of expectations, recognizing their significance empowers investors to make more informed decisions. Nevertheless, given the inherent unpredictability of financial markets, maintaining a flexible and adaptive approach to investment remains paramount.

Once the author has clarified the definition and fundamental concept of abnormal returns, the narrative pivots towards a detailed examination of their calculation approaches. Emphasizing precision, the author directs attention to Table 1, a comprehensive scheme that showing different methods of calculation of abnormal returns. Each approach is meticulously outlined, accompanied by a thorough analysis of its respective advantages and disadvantages. By meticulously dissecting these approaches, the author endeavors to equip readers with a

nuanced understanding of how abnormal returns can be accurately assessed within the realm of financial analysis.

Table 1

Advantages and disadvantages of different metrics for calculations the abnormal returns

Metrics	Formulas	Advantages	Disadvantages
Abnormal return (AR)	$AR_{it} = R_{it} - E(R_{it})$, where AR_{it} - abnormal return for security i on day t, R_{it} - actual return for security i on day t, $E(R_{it})$ - expected return for security i on day t	Provides potential insights for the future performance, simple and suitable for the analysis of many events.	Relies on limited historical data, ignores cumulative effect, assumes market efficiency assumption, limited to the timeframe.
Average abnormal return (AAR)	$AAR = \frac{1}{N}\sum_{i=1}^{N} AR_{it}$, where AAR - average abnormal return, n - number of days in the period, AR_{it} - abnormal return for security i on day t	Provides potential insights for the future, benchmarking, and it is risk adjusted.	Relies on limited historical data, short-term focuses, assumes market efficiency assumption, limited to the timeframe.
Cumulative Abnormal return (CAR)	$CAR_i(T_1, T_2) = \sum_{t=T_1}^{T_2} AR_{it}$, where day T_1 - the initial time period, T_2 - the final time period, AR_{it} - abnormal return for security i on day t	Provides potential insights for the future, show the cumulative effect, evaluates long-term performance.	Relies on limited historical data, is sensitive to chosen event window, assumes the constant expected returns, limited to the timeframe.
Cumulative Average Abnormal return (CAAR)	$CAAR_i(T_1, T_2) = \frac{1}{N}\sum_{i=1}^{N} CAR_i(T_1, T_2)$, where $CAAR_i$ - Cumulative Average Abnormal Return up to day t, n - number of days in the period	Provides potential insights for the future, smoothing of an asset`s abnormal returns, simplifies the interpretation, evaliates long-term performance.	Relies on limited historical data, concealment of short-term volatility, assumes the constant expected returns, limited to the timeframe.
Mean Adjusted return model (MAR)	$E(R_{it}) = R_i$, where $E(R_{it})$ - Expected return for security *i* on day *t*, R_i- actual return for security *i*	Provides potential insights for the future, simplifies, does not have alpha, and beta calculations.	Relies on limited historical data, short-term focus, assumes expected return is equal to the market return, limited to the timeframe.

Source: Compiled by the author based on the works by Barone (2023); Yosaf et.al (2022); Kolari and Pynnönen (2010).

As it can be seen, there are a lot of similarities and differences between those metrics. All of the methods contain several common similarities. One of them is the potential insights for the future. Basically, it means that after calculation and analysis of the abnormality for some events like wars, conflicts, pandemics, the investors may have insights into how to invest his or her money during that kind of events in the future. The second similarity is that all of these methods are used for the measurement of abnormal returns in the event studies. The last but not least similarity is that all of these metrics are expressed in the percentage terms, which makes them comparable and after the calculations of the abnormality, the analyst can compare the results in order to make the conclusion. In addition to that, all of the methods are limited to historical data, and they have the limitation of the timeframe. These two similarities are also the drawbacks of these methods.

There are also some differences. It should be mentioned that Abnormal returns (ARs), and Average Abnormal returns (AARs) may not be so useful in long-term event window. They are better in short-term evaluation because they provide immediate influence on the event. That is different to Cumulative Abnormal returns (CARs) and Cumulative Average Abnormal returns (CAARs). These methods are more used for long-term evaluation, and they are less suitable for the short-term period. The mean-adjusted return model is a statistical approach that can be applied to both periods. This approach is often used, when it is needed the adjust for overall market changes to assess how a stock`s returns differ from expected.

The author made simple explanation of the formulas to the readers. The easiest way to think about formulas is that Abnormal Return (AR) is the deviation of the actual return from the expected return for a single security at a specific time, such as when a stock's actual return was 10% but the expected return was 8%, resulting in an $AR = 10\% - 8\% = 2\%$. Average Abnormal Return (AAR) extends this concept to multiple securities, averaging their ARs at a specific time. For instance, if the ARs of three stocks on a particular day were 2%, -1%, and 3%, the AAR would be $\frac{1}{3} \times (2\% - 1\% + 3\%) = 1.33\%$.

Cumulative Abnormal Return (CAR) sums up the ARs of a single security over a period of time, like when the ARs of a stock over three days were 2%, -1%, and 3%, resulting in a CAR of $2\% - 1\% + 3\% = 4\%$. Cumulative Average Abnormal Return (CAAR) averages the CARs of multiple securities over a period of time. For example, if the CARs of three stocks over a period of time were 4%, 2%, and 6%, the CAAR would be $\frac{1}{3} \times (4\% + 2\% + 6\%) = 4\%$.

The Mean Adjusted Return Model estimates the expected return of a security as its historical average return. For example, if a stock's returns over the past five years were 10%, 12%, 8%, 11%, and 9%, the MAR would be $\frac{1}{5} \times (10\% + 12\% + 8\% + 11\% + 9\%) = 10\%$. These formulas are used in event study methodology to measure the impact of an event on the performance of securities, with the choice of formula depending on the specific research question and available data.

To conclude, there are different methods for the measurement of stock abnormal returns with its advantages and disadvantages. These methods are used in different situations in order to measure abnormal returns. The main idea, why investors calculate these abnormal returns is that they rely on historical data to forecast the future. The investors look at different assets during unstable events in order to make better investing decisions in the future. In the next part, the author discusses the effects of external shocks on the stock market.

1.2. The effects of external shocks on the stock returns

An external shock is an unexpected event that leads to a substantial change in the economy. Examples of external shocks include geopolitical events, technological advancements, policy changes, or other exogenous factors that can disrupt the economy. These shocks can provide the benefits for some specific sectors and vice versa. (Borsekova et al., 2018)

External shocks, such as major economic, political, or technological events, can have significant impacts on the stock market. Investors closely monitor how these shocks might affect the sales and financial performance of individual companies, and adjust their expectations and investment decisions accordingly. The investors make diferent scenarios for the companies during the shocks and stocks react differently eventually. Figure 1 illustrates these scenarios, highlighting the whole process how external shocks impact the stock abnormal returns.

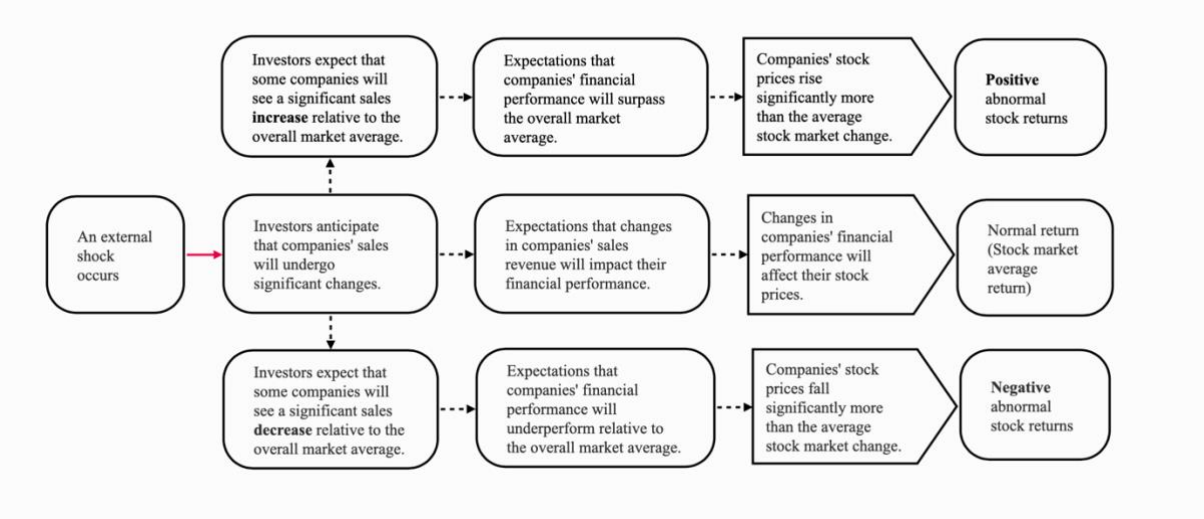

Figure 1. Impact of investor expectations on stock prices during external shocks
Source: Compiled by the author with the help of M. Kantšukov

In the face of an external shock where investors foresee certain companies experiencing a significant surge in sales compared to the market average, they expect these companies to outperform financially. This anticipation results in the stock prices of these companies rising notably more than the overall market change, leading to positive abnormal stock returns.

This phenomenon is often referred to as anticipatory stock movements. Investors anticipate future events or changes in a company's performance, such as increased sales due to an external shock, and adjust their valuations accordingly. (Schleicher et al., 2007)

In a scenario where investors anticipate certain companies facing a considerable decline in sales compared to the market average due to an external shock, they expect these underperforming companies to be behind financially. Consequently, the stock prices of these companies drop significantly more than the average stock market change, resulting in negative abnormal stock returns.

Conversely, when an external shock occurs, and investors predict substantial changes in companies' sales relative to the market, the stock prices of these companies adjust to reflect the expected financial impact. This adjustment aligns the stock prices with the overall market movement, resulting in a normal return that mirrors the market's behavior.

The author is trying to make the point that external shocks have the impact on the stock market, but some sectors can benefit from these events. It is important to know, which stocks brought abnormal returns to the investors during the external shocks in order to make better diversification and earn more returns in the future or vice versa to know the stocks that underperformed and not to invest in them during the time of instabilities. In the further text,

the author will explain why he thinks that US cybersecurity sector could benefit during COVID-19 and Russo-Ukrainian conflict.

Millions of people started thinking about the change of their current workplace to the remote one during COVID-19. The lockdowns overturned all the conventional understanding about the traditional workplaces. (Al-Habaibeh et al., 2021)

The new approach of the security was needed. In the cybersecurity sector, the zero-trust architecture became more famous during the COVID-19. The previous hub and spoke architecture was outdated and could not defend the employees, who worked from home. The main concept behind the zero-trust architecture is that the company should not trust, but also verify. It applies to everything like applications, identities, files and so on. (Buck et al., 2021)

The companies started rethinking about their previous cybersecurity systems and began applying the zero-trust architecture. That was the breakthrough in the cybersecurity sector. COVID-19 was the catalyst for the adoption of new technology. Thus, the author think that it boosted the financial performance of cybersecurity companies during that time because it increased the demand for new solutions.

The author downloaded the historical, financial data from official annual reports of the companies that operates in cyber security sector and calculated revenue growth rates. The list of the companies consists of 20 ones. The author will also use this list in further empirical part. The revenue growth rates periods were based on the official dates of the external shocks.

Despite the challenging economic landscape, Crowdstrike emerges as a leader performer with an impressive revenue growth rate of 81.64%, indicating its resilience during the pandemic. Similarly, Datadog's impressive growth of 70.48% underlines the increasing demand for security and analytics solutions as businesses rapidly transitioned to remote workplaces.

Zscaler's strong growth of 56.07% reflects the accelerated adoption of cloud security and VPNs replacement. Cloudflare's growth rate of 52.28% highlights the importance of its cloud-based and application security to solve the problem with remote workers. Google's solid growth at 41.15% amidst the pandemic showcases the diversified nature of its business, spanning various sectors that experienced increased demand during this period.

Microsoft's growth rate of 17.53% indicates its ability to navigate the challenges of the pandemic while maintaining steady progress across its suite of products and services including Microsoft Defender, cyber security solution. Despite the overall positive growth trends, Cisco's relatively lower growth rate at 1.05% suggests the impact of pandemic-

induced disruptions on certain sectors of its business. To prove that point, the author proposes to look at Figure 2.

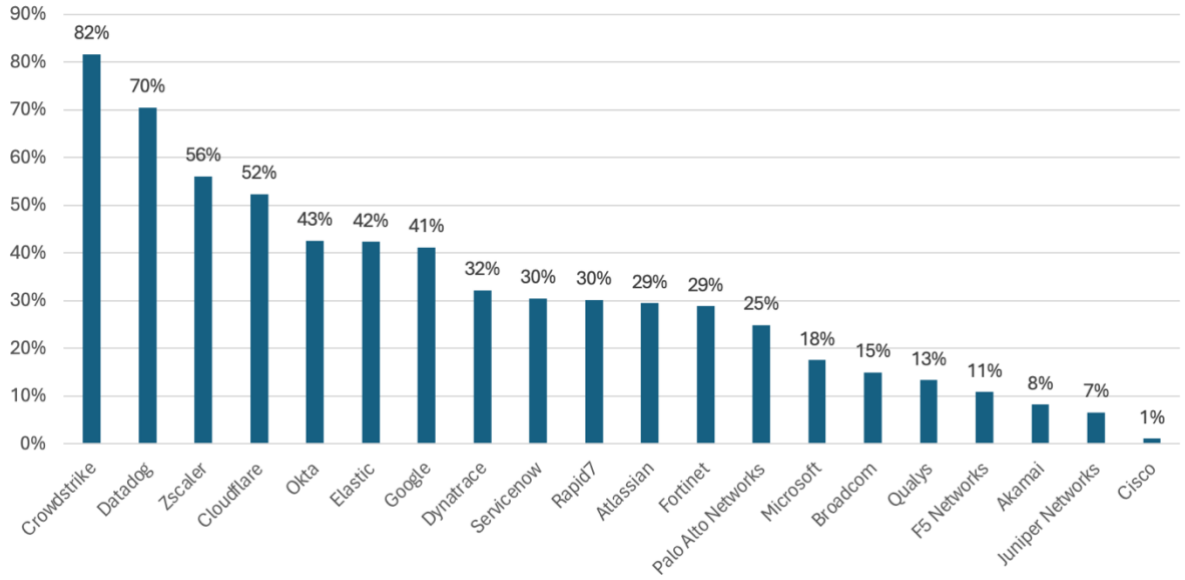

Figure 2. Sales revenue growth 2020-2021 of US cyber security companies
Source: Compiled by the author

Comparing the revenue growth rates from 2020-2021 to those from 2022-2023, we observe notable shifts in the cybersecurity landscape. In the earlier period, companies like Crowdstrike, Zscaler, and Cloudflare experienced enormous growth rates, indicating the increasing demand for cybersecurity solutions during the COVID-19 pandemic. However, in the latter period, while still maintaining positive high growth, it has decreased.

Crowdstrike saw its growth rate decline from 81.64% to 54.40%, suggesting a slowdown in the rapid adoption of its cybersecurity offerings. Zscaler's growth rate decreased from 56.07% to 48.22%, reflecting a little less drop in the demand for cloud security solutions. Cloudflare also experienced a decrease in growth rate from 52.28% to 32.97%, indicating significant drop. These shifts may suggest stabilized demand for cybersecurity solutions because of remote work trend. Nevertheless, geopolitical tensions like the Russo-Ukraine conflict likely bring new cybersecurity challenges. To prove that point, the author proposes to look at Figure 3.

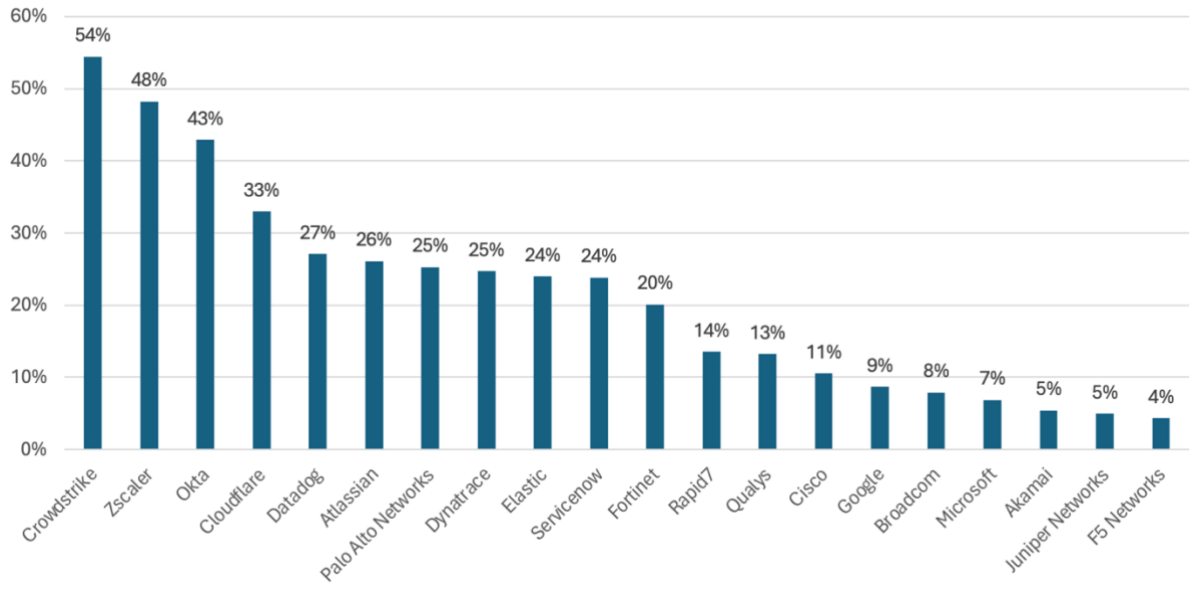

Figure 3. Sales revenue growth 2022-2023 of US cyber security companies
Source: compiled by the author

Companies like Okta, Palo Alto Networks, and Datadog maintain high growth. The Demand remains strong for identity management, network security, and cloud monitoring solutions, signaling stability in cybersecurity with pockets of strength.

In conclusion, external shocks such as the COVID-19 pandemic and geopolitical conflicts have significant impacts on various sectors of the economy, where some companies or sectors experiencing positive abnormal returns while others suffer losses. It becomes evident that the cybersecurity sector stands out as a beneficiary during such turbulent times. The transition to remote work, assisted by the pandemic, led to an increased demand for cybersecurity solutions, particularly those that develop zero-trust architectures and cloud-based security products. Furthermore, the emergence of geopolitical tensions like the Russo-Ukraine conflict introduced new cybersecurity challenges, highlighting the continued importance of the sector.

1.3. The overview of previous studies on stock abnormal returns during crises – the case of COVID-19 pandemic and Russo-Ukranian conflict

In this subchapter, the author is going to review studies that were previously conducted on similar topics by other authors. For analysis, the author selected studies that, in addition to the topic related to abnormal returns, also covered periods such as the COVID-19 pandemic and the Russo-Ukrainian conflict. This choice of research studies is due to the fact that in the study the author plans to analyze the abnormal returns of companies in the

cybersecurity sector precisely taking into account events such as the COVID-19 pandemic and the Russo-Ukrainian conflict. The author analyzes five different empirical studies, find similarities and differences between them and shows the methodology followed by the authors of the studies. These five empirical studies is divided into two groups, the first two studies are related to the COVID-19 pandemic and the stock market's response to it. Three other studies focus on the stock market's reaction to the Russo-Ukrainian conflict. Before analyzing each study individually, the author would like to present Table 3, where one can briefly familiarize himself/herself with the basic information characteristic of each analyzed study.

Table 3

The results of previous studies on abnormal stock returns during COVID-19 pandemic and Russo-Ukrainian conflict

Authors	The effect	Main results
Chen and Yen (2021)	Negative abnormal returns of metal stocks	Announcement of Quantitative Easing (QE) led to abnormal returns in some sectors during COVID-19 pandemic.
Mazur et al. (2021)	Negative abnormal returns of petroleum, real estate, entertainment, and hospitality stocks	The abnormal returns were identified in certain sectors on black Monday, black Tuesday, and black Monday II.
Umar et al. (2022)	Positive abnormal returns for clean energy stocks	Clean energy sector experienced positive abnormal returns after the war. Metal markets also showed positive abnormal returns.
Martins et al. (2023)	Negative abnormal returns for banking stocks	Banks with exposure to Russia had more negative stock returns.
Nerlinger & Utz (2022)	Positive abnormal returns of energy stocks	Energy sector stocks experienced positive cumulative abnormal returns during the Russo-Ukraine conflict, based on CAAR analysis of 1630 energy firms starting from February 24, 2022.

Source: Compiled by the author

The first study was conducted by Chen and Yen (2021) on the title of "Global financial crisis and COVID-19: Industrial reactions". The authors supposed that the quantitative easing (QE), which was announced and implemented by the FED after the COVID-19 pandemic could bring abnormal returns in stocks of some sectors. Quantitative easing is the monetary policy strategy that stimulates economy by two main instruments:

decreasing interest rates, and increasing its central banking balance, in other words, printing the money (Matousek et al., 2019). This monetary policy is usually used after some crisis, when the economy falls, and the citizens of some countries suffer. The assumption of these two authors is very reasonable since the announcement of the QE can be the reason for a rally on the stock market. In their empirical study, they calculated Cumulative Abnormal Returns (CARs) for the 49 industries in the list. In addition to the calculation, they chose different timeframes. The CARs of 49 industries after zero, ten, thirty and sixty days after the first announcement of the QE. These authors also analysed not only the effect after the announcement of the QE, but also the effect of the COVID-19 pandemic and the financial crisis in 2008. The results were pretty obvious, that these two events negatively influenced the financial markets, but some of the industries managed to perform better. In the first study, the authors used CARs in their empirical part and found out that the announcement of the QE was some kind of salvation to some particular industries, which brought abnormal returns to the investors.

The second empirical study was made by Mazur et al. (2021) on the title of "COVID-19 and the March 2020 stock market crash. Evidence from S&P1500". This study found pretty much the same result from the stock market perspective. There were some industries, which performed better, but not all of them. The author will focus on the calculations and how they were done. The authors of this study did not calculate the CARs as the previous study. Instead of that, they used mean-adjusted return model. Mean-adjusted return model is used for the evaluation of the performance of an investment thanks to the comparison of its returns to market index. They tried to find the abnormality by using this model and found that some particular industries performed better on the black Monday, black Tuesday, and black Monday II.

By comparing the studies, the author would like to highlight some similarities and differences characteristic of the two quite similar studies. One of the similarities can be found in that two of these studies used event-study methodology. They compared the abnormal returns from different industries during COVID-19, financial crises, and specific dates. Event studies are crucial in the calculation of the abnormality of the returns. The main reason for it is that they isolate the impact of specific events on asset prices. In addition to the isolation, event studies help with the comparison across different events. After the comparison, the investors or portfolio managers can build new assumptions knowing how different events influence the stock market. It doesn't always happen that some events bring only negative

results. For example, the announcement of the QE is perceived positively by the investors and during that time some industries can bring positive abnormal returns. However, both of these studies showed the negative effect of the COVID-19 pandemic and that the stock market reacted negatively to this kind of event.

After understanding of the similarities, the author would like to write about the differences between these two studies on the stock market reaction during COVID-19. The main difference between these studies is their method for the calculation of abnormal returns. In the first study, the authors used CARs, but in the second one mean-adjusted return model was spelled out. The main reason for that is the timeframe. The first study used more days for the calculations of the abnormal returns. The second study used just separate days. For the analysis of just one day, Cumulative Abnormal Returns (CARs) might be less suitable because CARs are typically used to assess abnormal returns cumulatively over a longer period. CARs involve a cumulative calculation, they are more appropriate for studying the impact of events that lasts over multiple days. Another difference is the results of the sectors that performed better and brought abnormal returns, in the second study there was a sector like software, that was not mentioned in the first one.

As it was previously mentioned, the author analyzes the second group of empirical studies that were connected to the Russo-Ukrainian conflict and the stock market reaction to it. The first study was made by Umar et al. (2022) on the title of "Impact of Russian-Ukraine war on clean energy, conventional energy, and metal markets: Evidence from event study approach". In this research, the authors assumed that the investors anticipated the potential growth in the clean energy sector during different timeframes after the war. The assumption is pretty solid since after the war started, the investors tried to find companies that provide alternative energy sources. Consequently, the companies in this sector could earn more profits and the stock prices should have gone up. Actually, that was the case and they found that the clean energy sector earned abnormal returns. In this study, the authors used slightly different method because they calculated Cumulative Average Abnormal Returns (CAARs) and Average Abnormal Returns (AARs). AARs represent the average abnormal returns for each day within an event window, while CAARs show the cumulative average abnormal returns over a series of time periods, providing a broader perspective on the impact of events on financial instruments. They found that abnormal returns were positive significant only in the clean energy and metal markets. The authors calculated these returns within 27-day event window from t-5 to t+21 days.

The second empirical study was made by Martins et al. (2023) on the topic of "Russia-Ukraine conflict: The effect on European banks' stock market returns". In this study, the authors calculated the CARs for 100 largest European banks. The results of these study showed that the banking sector reacted negatively to the war. The reason for that they assumed the people would try to spend less and take their deposits from the banks. In almost every unclear situation, people want to hold their money in cash. The study also showed the banks that had large exposure to Russia had more negative stock returns than the banks that did not have that exposure.

The third study that the author studied is the work of Nerlinger & Utz (2022) on the topic "The impact of the Russia-Ukraine conflict on energy firms: A capital market perspective". The authors explored the impact of the Russian invasion of Ukraine on energy firms' stock prices. In this study, the authors also calculated AAR and CAAR by taking 1630 firms from energy sector and an event window of 40 days (20 days before the event and 20 days after). Findings indicated that energy companies experienced positive cumulative average abnormal returns around the event date. Specifically, investors seemed to expect profits in conventional energy sectors, such as uranium technology. Although one might expect renewable energy companies to benefit the most from the event, challenges like long planning horizons for energy transitions have influenced the results.

All three studies use an event study approach to analyze the impact of the Russo-Ukrainian conflict on different sectors and employ the concepts of AAR and CAAR to measure the impact on stock market returns. Each study focuses on specific sectors, however the event windows vary among them. The results also differ across studies, since the first study found positive abnormal returns in clean energy, the second found negative impacts on European banks' stock market returns, and the third found positive cumulative average abnormal returns for energy companies, particularly in conventional energy. While the approaches and measurements are similar, each study examines different sectors and draws different conclusions based on the impact of the conflict on those sectors.

To summarize the information above, the author can highlight several main aspects. All five empirical studies were conducted via event study methodology. This is the most effective way how to calculate positive or negative abnormal returns to some specific events. By the comparison of different events and their effects on market reactions, investors or portfolio managers would be able to diversify their portfolios and save money during various crises. In some particular cases, the CARs should be calculated, in others CAARs, AARs or

mean-adjusted return model. After analyzing these five studies, the author decided to use event study methodology in the thesis in order to compare US cybersecurity returns to the NASDAQ composite index. Since, to the best of the author`s knowledge nobody has ever analyzed the abnormality of US cybersecurity stocks during the first month of COVID-19 and Russo-Ukrainian conflict, the author will try to fill the existing research gap.

2. Abnormal returns of US cybersecurity companies – empirical analysis

2.1. Methodology and data

In this sub-chapter, the author explains in detail the research approach that is going to be used. Also, the author would like to mention that this empirical analysis follows the approach applied by Rustambekova (2023). The study applies a quantitative approach to analyze the abnormal returns of US cybersecurity stocks over the two event windows it examines. The first event window that the author examines is the first month after the announcement of the COVID-19 pandemic and the beginning of the Russo-Ukrainian conflict. This period was chosen by the author because it allows him to cover a sufficiently long period of time, thanks to which the author can, to a certain extent, isolate the effect of the beginning of two events from other factors. For example, the release of financial statements of companies. The second event window will be precisely the day when each of the events began, namely March 11, 2020, when the start of the COVID-19 pandemic was announced and February 24, 2022, when a full-scale conflict between Russia and Ukraine began. This research method is called Event Study Methodology and it was chosen by the author to capture the immediate market reaction and evaluate the potential positive abnormal returns of US cybersecurity stocks.

In terms of selecting companies, the author researched over 100 companies to come up with a list of companies operating in the cybersecurity sector. This list includes 20 companies from the United States, since this country has the most developed cybersecurity market and the vast majority of companies in this sector are based in this country. However, the author would like to specifically note that the list includes companies both completely focused on providing cybersecurity services, and those who only partially work in this area, for example, companies such as Microsoft and Google. The historical data for this study will be taken from a reputable financial database, namely Bloomberg Terminal. Historical stock price data for the US cybersecurity companies will be collected over the 2 specific periods described earlier to assess the performance of the cybersecurity sector during the two selected events. After collecting the data, the author plans to download all historical data from the

Bloomberg terminal into Excel in order to calculate the daily returns of these stocks for each day within a month after the start of each of the events. After this, all the results obtained will be compared by the author with 2 indices - the NASDAQ and S&P 500 indices, for which the author will also calculate daily changes. This comparison will reveal whether abnormal returns took place both throughout the entire month and on a specific day of the event.

Identifying abnormal returns of 20 selected US cybersecurity stocks will provide insight into the sector's performance during crises. The choice of two indices for comparison is also determined by certain factors. The NASDAQ index includes leading technology companies, making it a suitable benchmark for evaluating the performance of US cybersecurity stocks. By comparing the abnormal returns of cybersecurity stocks to the NASDAQ index, the author can evaluate how the cybersecurity sector performed relative to the broader technology market during periods of crisis. In turn, identifying abnormal returns for cybersecurity stocks relative to the S&P 500 can give insight into how the sector compares to the overall US market. If cybersecurity stocks exhibit positive abnormal returns relative to indices, this may indicate that investors perceive cybersecurity companies as relatively safer investments during times of geopolitical tension or economic uncertainty. On the other hand, if a cybersecurity stock exhibits negative abnormal returns relative to indices, it may indicate that investors are less optimistic about the future of the cybersecurity sector compared to other stocks.

After identifying the abnormal returns for each event in comparison with the 2 indices in each of the time periods, the author plans to turn to statistical research to determine whether the obtained results after performing the calculations are statistically significant. The author's statistical test will be the Wilcoxon signed rank test, which is used to test differences between related pairs of data. It allows to determine whether differences between paired observations are significant when the data does not follow a normal distribution or the sample is too small. For a more visual representation of the main steps that will be taken by the author in the empirical part of the study, the author compiled Figure 3.

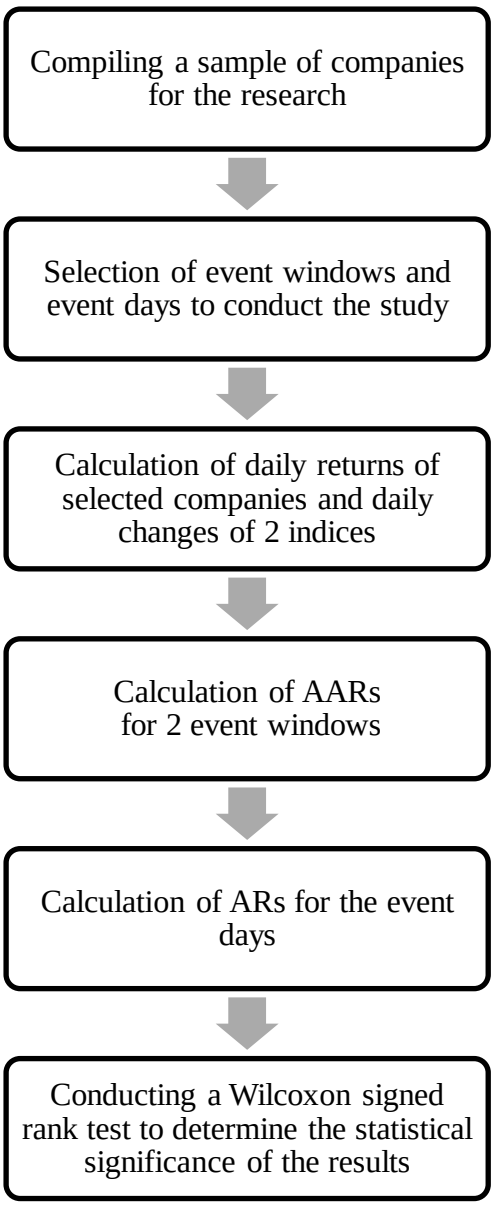

Figure 3. The main steps of the empirical part of the thesis

Source: Compiled by the author

The author is confident that strict adherence to the drawn-up plan for the empirical part of the study, will lead to achieving the research aim of the study. However, the author understands that following the written plan cannot guarantee the expected results, namely the identification of the statistical significance of the results. In the process of research, the author may encounter some difficulties, for example, due to the fact that the list of selected companies is limited to 20 companies. Next, the author would like to explain why these 20 companies were chosen.

The companies were selected based on their importance and influence in the US cybersecurity industry. Because the author's research focuses on the American market,

companies listed on US stock exchanges that specialize in cybersecurity were selected for inclusion in the study. The list of companies includes both large corporations and smaller organizations focused on innovative approaches of cybersecurity. At the same time, the author would specifically like to note that not all of the selected companies deal exclusively with cybersecurity. For example, such giant corporations as Google or Microsoft were also included in the study, despite the fact that cybersecurity is not their main area of activity. However, these organizations have departments that are directly related to cybersecurity.

The author's chosen companies in the US cybersecurity sector showcase diverse strategies for safeguarding data and networks. Analyzing them amidst the COVID-19 pandemic and the Russo-Ukrainian conflict can reveal trends in stock behavior during global crises. To assist readers in understanding the author's selected companies, a table has been created. This table provides information on the companies, including their stock exchange listings and approximate market capitalization as of April 1, 2024. Detailed information can be found below in Table 4.

Table 4

List of companies selected for research

Company name and ticker	Market capitalization in U.S. $ as of 01.04.2024	Stock Exchange
1. Microsoft Corporation (MSFT)	3.15T	NASDAQ
2. Alphabet Inc. (GOOGL)	1.93T	NASDAQ
3. Broadcom Inc. (AVGO)	625.73B	NASDAQ
4. Cisco Systems, Inc. (CSCO)	202.62B	NASDAQ
5. ServiceNow, Inc. (NOW)	157.52B	NYSE
6. Palo Alto Networks, Inc. (PANW)	90.28B	NASDAQ
7. CrowdStrike Holdings, Inc. (CRWD)	77.3B	NASDAQ
8. Fortinet, Inc. (FTNT)	51.75B	NASDAQ
9. Atlassian Corporation Plc (TEAM)	50.16B	NASDAQ
10. Datadog, Inc. (DDOG)	40.87B	NASDAQ
11. Cloudflare, Inc. (NET)	32.3B	NYSE
12. Zscaler, Inc. (ZS)	28.79B	NASDAQ
13. Okta, Inc. (OKTA)	17.32B	NASDAQ
14. Akamai Technologies (AKAM)	16.57B	NASDAQ
15. Dynatrace, Inc. (DT)	13.54B	NYSE
16. Juniper Networks, Inc. (JNPR)	11.93B	NYSE
17. F5, Inc. (FFIV)	11.16B	NASDAQ
18. Elastic N.V. (ESTC)	10.14B	NYSE
19. Qualys, Inc. (QLYS)	6.19B	NASDAQ
20. Rapid7, Inc. (RPD)	3.05B	NASDAQ

Notes. Capital T - trillions of dollars; capital B - billions of dollars

Source: Compiled by the author

As can be seen from Table 4, the list consists of 20 companies specializing in cybersecurity and/or related to this industry. Each company name is assigned a ticker symbol in accordance with the ticker symbol with which the shares of these companies are traded on exchanges. In the future, the author will indicate only the company ticker. The companies are sorted according to their market capitalization as of April 1, 2024. Most of the companies on the list are traded on the NASDAQ exchange, which is known for its technology companies, while only 5 companies chose to list on the NYSE. The preference of the NASDAQ exchange by most companies may seem strange to a reader not familiar with this topic, since the NYSE is an older exchange with a very long trading history. In fact, the preference for cybersecurity companies to list on NASDAQ may be explained by the fact that NASDAQ has historically specialized in technology and innovative companies, making it attractive to cybersecurity firms. This exchange provides convenient listing conditions aimed at high-tech and high-growth companies, including flexible listing requirements and lower listing costs.

NASDAQ also has a reputation as an exchange for companies that are at the forefront of technology and innovation, which fits well with the profile of cybersecurity companies. The NASDAQ is known for its higher volatility than the NYSE, which attracts investors interested in rapid growth and innovation. Companies that choose NASDAQ gain access to a broader audience of investors who are actively interested in the technology and innovation sector. This can lead to greater liquidity and potential for share price growth. Thus, NASDAQ's preference among cybersecurity companies indicates their focus on innovation and high growth potential, as well as their desire to work with investors interested in these aspects.

Also interesting is the fact that the companies selected by the author vary greatly in market capitalization. The range of market capitalization among the selected companies is quite wide, from $3.05 billion (RPD) to $3.15 trillion (MSFT), that is, if one compare the MSFT and RPD companies, that one can say that the MSFT company is worth more than 1000 times more, which is a huge difference.

The author purposefully selected companies with different capitalizations so that the conclusions from the research reflected both large corporations and small and medium-sized companies. The companies on the list include well-known tech industry leaders such as Microsoft (MSFT), Google (GOOGL), Cisco (CSCO), as well as younger and more dynamic companies such as CrowdStrike (CRWD) and Zscaler (ZS). As the author mentioned earlier, the companies on the list span various segments of cybersecurity and related industries,

including network security (AKAM), cybersecurity consolidator (PANW), security software (CRWD), and network technology (CSCO). This diversity of companies will allow the author, regardless of the market capitalization of the companies, explore the effect of crises such as the COVID-19 pandemic and the Russo–Ukrainian conflict on the cybersecurity sector.

2.2. Results and discussion

Once the reader is better acquainted with the companies participating in the author's study and better understands the reasons for including the companies in this study, the author believes it is reasonable to move on to the direct results of the calculations. However, before demonstrating the results of the calculations, the author would like to show what steps are behind each further number, which can be seen in subsequent tables. Since the author's ultimate goal was to assess whether a company showed abnormal returns after one month following the declaration of COVID-19 as a pandemic and the start of the Russo-Ukrainian conflict in comparison with the NASDAQ index, the following steps for each company and index were performed:

1. Entering data into Excel regarding the closing price of each of the 20 companies and the index from 11.03.2020 to 11.04.2020 and from 24.02.2022 to 24.03.2022.

2. Calculation of Daily return for each of the 20 companies and the index using the formula:

$$DR = \ln \frac{P_t}{P_{t-1}},$$

where DR equals daily stock/stock exchange return, Pt is the closing price of a stock on a current day and Pt-1 is the closing price of a stock on a previous day.

3. Calculation of Abnormal return according to the formula:

ARt = DRt – DRit,

where ARt is the abnormal return on day t, DRt is the stock return on day t and DRit is the index return on day t.

4. Calculate Average Abnormal returns (AARs).

After meticulously computing the Average Abnormal Returns (AAR) for every company during the initial month of two significant events - the onset of the COVID-19 pandemic and the eruption of conflict between Russia and Ukraine - the author endeavors to elucidate the findings. These findings have been meticulously collated and are meticulously detailed in Table 5 for comprehensive understanding and analysis.

Table 5
Two events AARs during 1 month compared to NASDAQ index

Company ticker	Average abnormal return (AAR) during COVID-19 (11.03.2020 – 11.04.2020)	Average abnormal return (AAR) during Russo – Ukrainian conflict (24.02.2022 - 24.03.2022)
1. AKAM	0.45%	0.39%
2. AVGO	-0.03%	0.07%
3. CRWD	1.00%	1.11%
4. CSCO	0.14%	-0.42%
5. DDOG	0.01%	-0.34%
6. DT	-0.47%	0.37%
7. ESTC	-0.30%	0.50%
8. FFIV	0.12%	-0.09%
9. FTNT	0.64%	0.36%
10. GOOGL	-0.21%	0.07%
11. JNPR	0.12%	-0.08%
12. MSFT	0.14%	-0.03%
13. NET	0.51%	0.97%
14. NOW	-0.41%	0.06%
15. OKTA	0.54%	-0.89%
16. PANW	0.41%	0.84%
17. QLYS	1.33%	0.72%
18. RPD	-0.05%	0.61%
19. TEAM	0.01%	-0.21%
20. ZS	1.24%	-0.50%

Source: Compiled by the author

After analyzing Table 5, the author can conclude that in the first month of the COVID-19 pandemic, 14 out of 20 companies showed positive abnormal returns compared to the NASDAQ index. This may indicate the benefits these companies have received due to increased cybersecurity needs as businesses and people shift to remote work and online activities. However, 6 out of 20 companies, such as AVGO, DT, ESTC, GOOGL, NOW and RPD showed negative AAR, which may indicate internal difficulties of the companies due to which they showed weaker performance in comparison with the NASDAQ index. Also, it is worth noting that two companies - AVGO and RPD lagged behind the NASDAQ index by only a little, 0.03% and 0.05%, respectively. Overall, most companies showed positive AARs during the pandemic, indicating the pandemic's favorable impact on cybersecurity stocks.

After one month from the start of the Russo-Ukrainian conflict, 12 out of 20 companies showed positive abnormal returns compared to the NASDAQ index, this is two companies less compared to the COVID-19 pandemic, but most companies still showed positive AAR. This effect can be explained by increased geopolitical tensions around the world, which have led to increased concerns in the field of cybersecurity and, as a result,

increased demand for cybersecurity services. For example, many companies around the world were concerned about the possible increase in cyber attacks such as phishing, fraud, infrastructure attacks and other forms of malicious activity that could be caused by this conflict. Particular attention was paid to protecting critical infrastructure, including energy, financial and communications systems. However, 8 out of 20 companies still showed negative AARs. Again, it should be noted that companies such as FFIV, JNPR and MSFT underperformed the index by just 0.09%, 0.08% and 0.03% respectively. However, the underperformance of some companies from the index can be explained by internal problems within the companies or weak financial statements released. For example, the ZS company on 24.02.2022 reported worse than experts' expectations, which on the next trading day brought down the share price by more than 17% (*Zscaler (ZS) earnings dates & reports,* 2022), which, as can be seen, resulted in a relatively weak month in comparison with the index. Overall, there has been mixed performance among companies during the conflict, some of which have benefited from increased attention to cybersecurity issues while others have struggled.

The findings from the Table 5 suggest that cybersecurity stocks have generally demonstrated resilience and adaptability during the pandemic and the Russo-Ukrainian conflict, with many showing positive abnormal returns. As discussed earlier, this indicates an increase in demand for cybersecurity services during these periods. The impact of events varied across companies, indicating that each company faced unique challenges and opportunities for growth. These results can help investors identify cybersecurity companies that are more resilient and potentially profitable during times of crisis.

After conducting research on whether the author's selected companies showed abnormal returns compared to the NASDAQ index, the author came up with the idea of comparing the same companies to a broader index, namely the S&P500 index. According to the author, comparing the abnormal returns of cybersecurity companies to the S&P 500 index, in addition to the NASDAQ index, can provide a broader understanding of the performance of these companies during the COVID-19 pandemic and the conflict between Russia and Ukraine. The NASDAQ index focuses primarily on technology companies, while the S&P 500 covers a broader range of industries, including financials, industrials and energy. A comparison with the S&P 500 will provide insight into how cybersecurity companies stand out among other non-tech industries.

Because the NASDAQ is more volatile due to the dominance of technology companies, and the S&P 500 has less volatility, looking at the returns of cybersecurity companies relative to a less volatile index may reveal more persistent or unusual trends. Also, since the S&P 500 is considered a representative index for the entire US market, a study of how cybersecurity companies performed during the 2-event period compared to the index may show better performance and higher abnormal returns compared to the NASDAQ index. Overall, such a comparison can provide a more complete picture of how cybersecurity companies perform in the context of the entire market, not just the technology sector. This can lead to a better understanding of the risks and opportunities of investing in this sector, as well as the development of more effective investment strategies.

To compare the returns of the same 20 companies, but only with a different index, the author used the same formula for calculating daily returns for companies and the S&P500 index as in a similar study with the NASDAQ index. Next, the author calculated the abnormal return for each of the companies in each of the two events and is ready to present the results of the research in Table 6.

Table 6

Two events AAR during 1 month compared to S&P 500 index

Company ticker	Average abnormal return (AAR) - COVID-19 (11.03.20 – 11.04.20)	Average abnormal return (AAR) - Russo – Ukrainian conflict (24.02.22 - 24.03.22)
1. AKAM	0.62%	0.50%
2. AVGO	0.14%	0.17%
3. CRWD	1.17%	1.21%
4. CSCO	0.31%	-0.32%
5. DDOG	0.17%	-0.23%
6. DT	-0.30%	0.47%
7. ESTC	-0.13%	0.61%
8. FFIV	0.29%	0.01%
9. FTNT	0.81%	0.47%
10. GOOGL	-0.04%	0.17%
11. JNPR	0.28%	0.02%
12. MSFT	0.31%	0.07%
13. NET	0.67%	1.07%
14. NOW	-0.24%	0.17%
15. OKTA	0.70%	-0.79%
16. PANW	0.57%	0.94%
17. QLYS	1.50%	0.82%
18. RPD	0.11%	0.72%
19. TEAM	0.18%	-0.10%
20. ZS	1.40%	-0.39%

Source: Compiled by the author

A study of the abnormal returns of cybersecurity companies relative to the S&P 500 index during the COVID-19 pandemic and the conflict between Russia and Ukraine showed interesting results. The abnormal returns of cybersecurity companies are higher compared to the S&P 500 than to the NASDAQ index. This may be due to the fact that the S&P 500 index includes a wider range of industries, not just the technology sector like the NASDAQ. Moreover, the figures are higher for absolutely each of the 20 companies and for both events. For example, CRWD posted abnormal returns of 1.17% during the COVID-19 pandemic and 1.21% during the Russo-Ukrainian conflict, compared to 1% and 1.11%, respectively, for the Nasdaq index. It is also worth noting that some companies, such as the already mentioned CRWD, as well as FTNT and QLYS, showed noticeably higher average abnormal returns during both events compared to both indices. This indicates that these companies may be more resilient or successful during such crises.

Another extremely interesting fact is that during the COVID-19 pandemic, only 4 companies showed a negative AAR in comparison with the S&P 500 index. Moreover, the most negative AAR is that of the DT company and is only -0.3%. While the most positive AAR during COVID-19 is for ZS with its 1.4%. If we compare the results obtained with the NASDAQ index, then during the same period there were 6 companies that showed a negative AAR. A similar trend is observed for the conflict between Russia and Ukraine. In comparison with the NASDAQ index, there were 8 companies that showed a negative AAR, and in comparison with the S&P 500 index there were only 5 such companies. During the conflict between Russia and Ukraine, the highest negative AAR was for OKTA and was -0.79%, and the highest positive AAR for CRWD and is 1.21%.

Overall, the study's findings suggest that cybersecurity companies can exhibit superior resilience and returns during crises, especially when compared to the overall market represented by the S&P 500. This makes the cybersecurity sector attractive to investors seeking assets with high returns and stability during unstable periods.

In addition to identifying the abnormal returns of shares of selected companies with the NASDAQ and S&P 500 index within a month after the event, the author believes that it would also be interesting to conduct a study on how the stocks changed directly in the days of the announcement of the COVID-19 pandemic and the outbreak of the conflict between Russia and Ukraine. To conduct such a study, the author plans to use Event Study Methodology. The author is convinced that this will be a good way to find out exactly how investors assessed the impact of two events on a stock, since ESM allows one to isolate the

impact of specific events on the share price of selected companies. This makes it possible to determine how news about the COVID-19 pandemic and the beginning of the Russo-Ukrainian conflict affected the price of shares of companies operating in the field of cybersecurity. The ESM methodology defines the exact time frame around events (in this case March 11, 2020 and February 24, 2022) for analysis. This helps assess the short-term impact of news on the stock market.

For this study, the author also chose to calculate the abnormal returns in comparison with the indices already known to the reader - NASDAQ and S&P 500. Below in Table 7, the author would like to demonstrate the results of the abnormal returns that were obtained in comparison with the NASDAQ index.

Table 7

Two events AR during event day compared to NASDAQ index

Company ticker	Abnormal return (AR) - COVID-19	Abnormal return (AR) - Russo – Ukrainian conflict
1. AKAM	5.48%	1.60%
2. AVGO	2.18%	-0.80%
3. CRWD	-4.58%	8.84%
4. CSCO	-3.39%	-2.85%
5. DDOG	-2.16%	3.35%
6. DT	-6.76%	1.27%
7. ESTC	-4.92%	7.84%
8. FFIV	-4.47%	-1.43%
9. FTNT	1.37%	7.25%
10. GOOGL	-0.69%	0.54%
11. JNPR	-0.62%	-1.95%
12. MSFT	-0.16%	1.60%
13. NET	1.98%	13.72%
14. NOW	-2.88%	5.59%
15. OKTA	0.66%	5.06%
16. PANW	-1.64%	8.88%
17. QLYS	0.51%	5.33%
18. RPD	1.16%	5.34%
19. TEAM	0.68%	3.68%
20. ZS	-4.72%	6.16%

Source: Compiled by the author

The results that the author obtained after conducting the study turned out to be quite interesting. Cybersecurity companies have had mixed results during the COVID-19 pandemic, with 13 companies (compared to just 6 on a monthly timeframe) reporting negative returns relative to the NASDAQ index. And this is even taking into account the fact that the NASDAQ index fell more than 4.5% that day, which is a significant drop for the index. However, some companies such as AKAM (5.48%) and NET (1.98%) showed positive

abnormal returns. However, many companies, including AVGO (-2.18%), CRWD (-4.58%), and CSCO (-3.39%), showed negative ARs. In general, at the beginning of the pandemic, many investors tried to withdraw their money from their accounts at brokerage firms due to the uncertainty that the pandemic could bring, which led to a decrease in market activity at the beginning of the pandemic. The author believes that this was one of the reasons why the shares of financially strong and stable companies fell sharply that day, without any reasons directly related to the companies.

The Russo-Ukrainian conflict had a positive impact on companies, reflected in a 3.4% increase in the index. CRWD (8.84%), FTNT (7.25%), NET (13.72%), and PANW (8.88%) saw significant positive returns due to heightened cybersecurity needs amidst geopolitical tensions. AVGO (-0.80%), CSCO (-2.85%), FFIV (-1.43%), and JNPR (-1.95%) were the only companies with negative abnormal returns, out of 20, on that day. Overall, 16 companies had positive abnormal returns compared to the index. All 20 companies saw their share values rise compared to the previous trading day's close. However, looking beyond the index comparison, in the month following February 24, 2022 (as shown in Table 5), 8 out of 20 companies experienced a negative Average Abnormal Return (AAR) compared to the NASDAQ index.

As with identifying abnormal returns over a one-month period, the author compared the abnormal returns of cybersecurity companies on the day of the event with the S&P 500 Index. The purpose of this analysis was to evaluate how cybersecurity companies reacted to two events compared to the overall market, not only in comparison with other technology companies that are included in the NASDAQ index. For clarity of the results, the author compiled Table 8.

Table 8

Two events AR during event day compared to S&P 500 index

Company ticker	Abnormal return (AR) - COVID-19	Abnormal return (AR) - Russo – Ukrainian conflict
1. AKAM	6.02%	3.51%
2. AVGO	-1.65%	1.10%
3. CRWD	-4.04%	10.74%
4. CSCO	-2.85%	-0.95%
5. DDOG	-1.63%	5.26%
6. DT	-6.23%	3.18%
7. ESTC	-4.38%	9.74%
8. FFIV	-3.93%	0.47%
9. FTNT	1.91%	9.16%
10. GOOGL	-0.15%	2.44%
11. JNPR	-0.08%	-0.05%

12. MSFT	0.37%	3.50%
13. NET	2.52%	15.62%
14. NOW	-2.34%	7.49%
15. OKTA	1.20%	6.96%
16. PANW	-1.10%	10.78%
17. QLYS	1.04%	7.23%
18. RPD	1.70%	7.24%
19. TEAM	1.21%	5.58%
20. ZS	-4.19%	8.06%

Source: Compiled by the author

In general, the results of this study show a similar trend that was observed when identifying abnormal returns in comparison with the NASDAQ index. During the COVID-19 pandemic, 12 companies showed negative abnormal returns compared to the S&P 500 index. This is 1 company less than compared to the NASDAQ index, as MSFT showed positive abnormal return compared to the S&P 500 index. It is also interesting to note that all companies showed improvement in their results in comparison with the NASDAQ index. However, this should no longer be news to the reader, since a similar trend was observed when the author compared the results for a monthly period. During the Russo-Ukrainian conflict, there is a more positive reaction from most cybersecurity companies, as compared to the NASDAQ index. However, this time only 2 companies showed negative abnormal returns. Moreover, companies such as NET (15.62%), PANW (10.78%) and CRWD (10.74%) showed the highest positive abnormal returns. 15 other companies also showed positive AR, although to a lesser extent. As with COVID-19, all companies improved their performance relative to the NASDAQ index.

The differences in abnormal returns for the two events suggest that cybersecurity companies respond differently to events depending on their nature and context. The Russo-Ukrainian conflict, unlike the pandemic, caused a more noticeable positive impact on cybersecurity stocks. This may be due to the increased demand for cybersecurity services around the world during the conflict.

After carrying out calculations aimed at identifying abnormal returns on stocks of selected companies in the cybersecurity sector over two time periods (one month and the event day), the author decided to conduct the Wilcoxon signed rank test. This test is nonparametric and is used to compare paired samples or related samples. In this case, the test was chosen because it compares differences in abnormal returns between two related samples: abnormal returns during the first month of pandemic and abnormal returns during

the first month of the conflict. Also, a nonparametric test is used due to the relative small number of companies selected by the author for the study.

Before conducting the actual test, the author decided to demonstrate descriptive statistics, which can be observed in Table 9.

Table 9
Descriptive Statistics of AAR compared to the NASDAQ index

	N	Minimum	Maximum	Mean	Std. Deviation
COVID19	20	-.004679	.01330	.0025999	.00506
CONFLICT	20	-.008940	.01112	.0017618	.00525

Source: Compiled by the author

Table 9 shows that the COVID-19 and Russo-Ukrainian conflict periods had similar characteristics in terms of minimum/maximum, mean and standard deviation of returns during 1 month timeframe. The mean values for the two periods are quite similar, indicating similar performance of cybersecurity firms during both events. Similar standard deviations indicate comparable volatility of returns between the two periods.

Before directly proceeding to the test, the author set the following hypotheses, which should be identified using the test.

H0: COVID-19 average abnormal returns of chosen stocks for one month period is equal to Russo-Ukranian conflict average abnormal returns of chosen stocks for one month period.

H1: COVID-19 average abnormal returns of chosen stocks for one month period is not equal to Russo-Ukranian conflict average abnormal returns of chosen stocks for one month period.

After putting forward the hypotheses necessary to conduct the test, the author would like to present the results of the test itself in Table 10.

Table 10
Wilcoxon Signed Rank Test with monthly data compared to the NASDAQ index

Wilcoxon Signed Rank Test	
Total N	20
Test Statistic	101.000
Standard Error	26.786
Standardized Test Statistic	-.149
Asymptotic Sig. (2-sided test)	.881

Source: Compiled by the author

In Table 10, the main value that the author would like to pay attention to is the Sig. value (asymptotic significance). The value is 0.881, which indicates that there is no statistically significant difference between the returns of the selected 20 companies during the COVID-19 pandemic and the Russo-Ukraine conflict, since the value is greater than 0.05.

Thus, the null hypothesis should be retained. The author's words are also confirmed in Table 11.

Table 11
Hypothesis Test Summary

Null Hypothesis	Test	Sig.	Decision
The median of differences between Covid19 and CONFLICT equals 0.	Related-Samples Wilcoxon Signed Rank Test	.881	Retain the null hypothesis

Source: Compiled by the author

The study results show that in the US cybersecurity industry there are no statistically significant differences in company returns compared to the NASDAQ index between the period of one month of the COVID-19 pandemic and the Russo-Ukrainian conflict. A Wilcoxon signed rank test showed that the median differences in cybersecurity company returns between the two periods are equal. These results can be explained by the fact that, looking at Table 5, there are certain similarities in how companies responded to the two events. There is also not much variation in the number of companies that responded positively (14 and 12 companies) to the onset of the pandemic and the start of the conflict. This might explain why the results did not show a statistically significant difference.

However, the author became interested in what result the same test would show if choosing not one month, but only one day, on which two events occurred. Just like with the previous test, the author decided to compare the event day of each event with the NASDAQ index. As with the previous test, the author first decided to demonstrate descriptive statistics, which can be observed in Table 12.

Table 12
Descriptive Statistics of AR compared to the NASDAQ index

	N	Minimum	Maximum	Mean	Std. Deviation
COVID19	20	-.06764	.05477	-.0137	.02964
CONFLICT	20	-.02855	.13720	.0395	.04263

Source: Compiled by the author

In this case, in contrast to the comparison of a period of 1 month, in Table 12 more significant differences between the 2 events can be seen. During the COVID-19 period, the average return was negative, consistent with Table 7, where 13 out of 20 companies reacted negatively to the event relative to the index. On the event day of the conflict, the average return was positive, which is also confirmed by the data from Table 7, where 16 out of 20 companies showed positive abnormal returns. The standard deviation of returns is higher

during the conflict period, indicating greater return volatility during this time compared to the pandemic period.

To conduct further research, the author needed to formulate hypotheses:

H0: COVID-19 average abnormal returns of chosen stocks for the event day is equal to Russo-Ukranian conflict average abnormal returns of chosen stocks for the event day.

H1: COVID-19 average abnormal returns of chosen stocks for the event day is not equal to Russo-Ukranian conflict average abnormal returns of chosen stocks for the event day.

After setting the hypotheses, the author proceeded to directly performing the test, the results of which can be observed in Table 13.

Table 13

Wilcoxon Signed Rank Test with event day data compared to the NASDAQ index

Wilcoxon Signed Rank Test	
Total N	20
Test Statistic	199.000
Standard Error	26.786
Standardized Test Statistic	3.509
Asymptotic Sig. (2-sided test)	<.001

Source: Compiled by the author

After running the test, the author suggests looking at the Asymptotic Sig. (2-sided test) value, which is less than 0.001, which means the result is statistically significant and that is why the author should reject the null hypothesis. Thus, the test results show that there are statistically significant differences between the two events event data compared to the NASDAQ index. A low asymptotic significance value indicates that the differences in the data are not random and are statistically significant. The author's words are also confirmed in Table 14.

Table 14

Hypothesis Test Summary

Null Hypothesis	Test	Sig.	Decision
The median of differences between Covid19 and CONFLICT equals 0.	Related-Samples Wilcoxon Signed Rank Test	<.001	Reject the null hypothesis

Source: Compiled by the author

The statistically significant results of this test can be explained by the fact that, as stated earlier, companies did react differently to the onset of the two events. If in the case of the event day for COVID-19, most companies showed negative returns compared to the NASDAQ index, then in the case of the event day of the beginning of the conflict everything

was exactly the opposite, which does not allow the author to say that there is no difference between the two events on the event day.

Separately, the author would like to note that the same tests were conducted in comparison with the S&P 500 index. However, the author decided not to include their results in this study, since the results obtained are similar to the results that the author showed on the example of comparing the abnormal returns of companies with the NASDAQ index. In particular, a comparison of abnormal returns between two events over one month compared to the S&P 500 index did not show statistically significant results. While a similar study but only on event day showed strong statistically significant results.

To conclude the results of the analysis, the author would like to note that the work on identifying the abnormal returns of selected companies during two events compared to two indices is a useful source of information for all investors who would like to understand in more detail how companies in the cybersecurity sector behave during periods of crisis. This study showed different results on abnormal returns of the cybersecurity companies. Practically all of them showed positive abnormal returns during the first month after the declaration of the shocking events. The results were different, when the author picked shorter event window to one day, when these shocks were announced. The results showed that just after the day of announcement, the stocks brought negative abnormal returns during first day of COVID-19, but they brought positive abnormal returns during first day of Russo-Ukrainian conflict.

However, the research conducted by the author also has certain limitations, since in the research the author selected not only companies that are 100% related to the cybersecurity sector, but also companies that are not engaged in this activity as their main activity. Vivid examples include Microsoft and Google, which the author also included in the list of 20 companies. However, the author believes that after reading the work, anyone wishing to understand companies in this sector in more detail will better understand the peculiarities of how events such as a pandemic or the outbreak of a major geopolitical conflict can affect the shares of these companies.

Conclusion

The Bachelor thesis explores the abnormal returns of US cybersecurity stocks in the context of the COVID-19 pandemic and the Russo-Ukrainian conflict. By examining how the market responds to external shocks, this research can offer valuable understanding of how stocks of the cybersecurity sector performs, providing insights for investors and industry participants.

The theoretical foundation of abnormal returns, as explored in this thesis, underlines the importance of measuring the impact of specific events on stock performance. By examining different approaches for calculating abnormal returns, investors can gain valuable insights into asset performance and make better decisions regarding investment strategies. The distinction between positive and negative abnormal returns highlights the nuances of asset performance in response to external shocks, offering an understanding of market dynamics in volatile conditions.

Anticipatory stock movements significantly influence market dynamics during external shocks. Investors adjust their valuations based on anticipated changes in company sales, leading to notable fluctuations in stock prices, resulting positive or negative returns in comparison with some index. If the investors do not anticipate that the impact of some event should lead to decline or surge in sales, some of the companies can bring normal return.

Through the analysis of previous studies, the author delved into the impact of external events on stock markets, highlighting the use of different methods of calculations such as Cumulative Abnormal Returns (CARs), mean-adjusted return models, Cumulative Average Abnormal Returns (CAARs), and Average Abnormal Returns (AARs). These studies revealed both positive and negative reactions in different sectors, emphasizing the importance of event-study methodology in understanding market behavior during crises.

Furthermore, the empirical analysis of abnormal returns in US cybersecurity companies has shed light on the performance of these companies following the events. By conducting an event study during the COVID-19 pandemic and the Russo-Ukrainian conflict, the study has provided empirical evidence of the impact of these events on stock returns within the cybersecurity sector. Following a quantitative approach, the research applies the Event Study Methodology to evaluate the abnormal returns of 20 US cybersecurity companies in comparison with NASDAQ, and S&P500 indicies during different event windows.

The results of this thesis show that during the first month from the day of announcement of COVID-19 pandemic and Russo-Ukrainian conflict were not statistically significant using Wilcoxon Signed Rank Test. On the contrary, the results of smaller event window, which is just the day of announcement show statistically significance and approve the H1 hypothesis. The author found that COVID-19 average abnormal returns of chosen stocks for the event day is not equal to Russo-Ukrainian conflict average abnormal returns of chosen stocks for the event day. The findings highlight the nuanced impact of external events

on cybersecurity stocks, particularly the event window and offer valuable insights for investors navigating turbulent market conditions.

At the beginning of the research, the author made two different assumptions such as increased financial performance of the US cybersecurity companies and technologies. The second assumption was that cybersecurity companies experienced increased demand for its solutions because of the technological shift from hub and spoke architecture to the zero trust one that started from the start of pandemic. That is why, the author believed these companies could bring abnormal returns, and the results of the empirical part confirmed that.

The author believes that there will be needed additional research, and hope that this research will be able to help to find any further effects of the cybersecurity companies during different shock events. Additional research can uncover further effects of cybersecurity companies during different shock events, future investigations could focus on analyzing longer event windows, comparing findings to other sectors, conducting the analysis on the European market, and integrating qualitative data to enhance understanding of cybersecurity stock performance in turbulent market conditions.

References

1. Aboody, D., Barth, M. E., & Kasznik, R. (1999). Revaluations of Fixed Assets and future firm performance: Evidence from the UK. Journal of Accounting and Economics, 26(1–3), 149–178. https://doi.org/10.1016/s0165-4101(98)00040-8
2. Al-Habaibeh, A., Watkins, M., Waried, K., & Javareshk, M. B. (2021). Challenges and opportunities of remotely working from home during covid-19 pandemic. Global Transitions, 3, 99–108. https://doi.org/10.1016/j.glt.2021.11.001
3. Barone, A. (2023, April 25). Abnormal return: Definition, causes, example. Investopedia. https://www.investopedia.com/terms/a/abnormalreturn.asp
4. Borsekova, K., Nijkamp, P., & Guevara, P. (2018). Urban resilience patterns after an external shock: An exploratory study. International Journal of Disaster Risk Reduction, 31, 381–392. https://doi.org/10.1016/j.ijdrr.2018.05.012
5. Boungou, W., & Yati, A. (2022). "The impact of the Ukraine-Russia war on world stock market returns." Economics Letters, 215, 110516. https://doi.org/10.1016/j.econlet.2022.110516
6. Buck, C., Olenberger, C., Schweizer, A., Völter, F., & Eymann, T. (2021). Never trust, always verify: A multivocal literature review on current knowledge and research gaps of zero-trust. Computers & Security, 110, 102436. https://doi.org/10.1016/j.cose.2021.102436
7. Capelle-Blancard, G., & Couderc, N. (2007). What drives the market value of firms in the Defense Industry? Review of Financial Economics, 17(1), 14–32. https://doi.org/10.1016/j.rfe.2007.02.001
8. Carvalho, C., Klagge, N., & Moench, E. (2011). The persistent effects of a false news shock. Journal of Empirical Finance, 18(4), 597–615. https://doi.org/10.1016/j.jempfin.2011.03.003
9. Chen, H.-C., & Yeh, C.-W. (2021). "Global financial crisis and COVID-19: Industrial reactions." Finance Research Letters, 42, 101940. https://doi.org/10.1016/j.frl.2021.101940
10. Fernandez De Arroyabe, I., Arranz, C. F. A., Arroyabe, M. F., & Fernandez de Arroyabe, J. C. (2023). Cybersecurity capabilities and cyber-attacks as drivers of investment in cybersecurity systems: A UK survey for 2018 and 2019. Computers & Security, 124, 102954. https://doi.org/10.1016/j.cose.2022.102954

11. Gao, L., Calderon, T. G., & Tang, F. (2020). Public companies' cybersecurity risk disclosures. International Journal of Accounting Information Systems, 38, 100468. https://doi.org/10.1016/j.accinf.2020.100468
12. Gyamfi-Yeboah, F., Ling, D. C., & Naranjo, A. (2012). Information, uncertainty, and behavioral effects: Evidence from abnormal returns around real estate investment trust earnings announcements. Journal of International Money and Finance, 31(7), 1930–1952. https://doi.org/10.1016/j.jimonfin.2012.05.013
13. Iyengar, K., Mabrouk, A., Jain, V. K., Venkatesan, A., & Vaishya, R. (2020). Learning opportunities from covid-19 and future effects on Health Care System. Diabetes & Metabolic Syndrome: Clinical Research & Reviews, 14(5), 943–946. https://doi.org/10.1016/j.dsx.2020.06.036
14. Kolari, J. W., & Pynnönen, S. (2010). Event study testing with cross-sectional - JSTOR. Event Study Testing with Cross-sectional Correlation of Abnormal Returns. https://www.jstor.org/stable/pdf/40961306.pdf?ab_segments=0%2Fbasic_search_gsv2%2Fcontrol&initiator=search-results
15. Liu, G., Fang, X., Huang, Y., & Zhao, W. (2021). Identifying the role of consumer and producer price index announcements in stock index futures price changes. Economic Analysis and Policy, 72, 87–101. https://doi.org/10.1016/j.eap.2021.07.009
16. Martins, A. M., Correia, P., & Gouveia, R. (2023). "Russia-Ukraine conflict: The effect on European banks' stock market returns." Journal of Multinational Financial Management, 67, 100786. https://doi.org/10.1016/j.mulfin.2023.100786
17. Mazur, M., Dang, M., & Vega, M. (2021). "Covid-19 and the March 2020 Stock Market Crash: Evidence from S&P1500." Finance Research Letters, 38, 101690. https://doi.org/10.1016/j.frl.2020.101690
18. Matousek, R., Papadamou, S., Šević, A., & Tzeremes, N. G. (2019). The effectiveness of quantitative easing: Evidence from Japan. Journal of International Money and Finance, 99, 102068. https://doi.org/10.1016/j.jimonfin.2019.102068
19. Nerlinger, M., & Utz, S. (2022). The impact of the Russia-Ukraine conflict on energy firms: A capital market perspective. Finance Research Letters, 50, 103243. https://doi.org/10.1016/j.frl.2022.103243
20. Petrosyan, A. (2023). Number of ransomware attempts per year 2022. Statista. https://www.statista.com/statistics/494947/ransomware-attempts-per-year-worldwide/

21. Petrosyan, A., & 10, O. (2023). Global average cost of a data breach 2023. Statista. https://www.statista.com/statistics/987474/global-average-cost-data-breach/
22. Rustambekova, S. (2023). ABNORMAL STOCK RETURNS OF PUBLIC GERMAN PHARMACEUTICAL COMPANIES DURING THE FIRST WAVE OF THE COVID-19 PANDEMIC. https://dspace.ut.ee/server/api/core/bitstreams/c96e1c93-ffed-4a70-a60c-dae3b3d792c1/content
23. Schleicher, T., Hussainey, K., & Walker, M. (2007). Loss firms' annual report narratives and share price anticipation of earnings. The British Accounting Review, 39(2), 153–171. https://doi.org/10.1016/j.bar.2007.03.005
24. Song, R., Shu, M., & Zhu, W. (2022). The 2020 global stock market crash: Endogenous or exogenous? Physica A: Statistical Mechanics and Its Applications, 585, 126425. https://doi.org/10.1016/j.physa.2021.126425
25. Umar, M., Riaz, Y., & Yousaf, I. (2022). "Impact of Russian-Ukraine war on clean energy, conventional energy, and metal markets: Evidence from event study approach." Resources Policy, 79, 102966. https://doi.org/10.1016/j.resourpol.2022.102966
26. Watts, R. L. (1978). Systematic 'abnormal' returns after quarterly earnings announcements. Journal of Financial Economics, 6(2–3), 127–150. https://doi.org/10.1016/0304-405x(78)90027-2
27. Yousaf, I., Patel, R., & Yarovaya, L. (2022). The reaction of G20+ stock markets to the Russia–Ukraine conflict "Black-swan" event: Evidence from event study approach. Journal of Behavioral and Experimental Finance, 35, 100723. https://doi.org/10.1016/j.jbef.2022.100723
28. Zscaler (ZS) earnings dates & reports. Investing.com. (2022). https://www.investing.com/equities/zscaler-inc-earnings

Resümee

USA küberturvalisuse aktsiate ebanormaalne tootlus COVID-19 pandeemia ja Venemaa-Ukraina konflikti ajal

Yaroslav Nedvyga

Bakalaureusetöö eesmärk oli hinnata USA turul kaubeldavate küberturbe ettevõtete aktsiate ebanormaalseid tootlusi pärast COVID-19 pandeemia ja Ukraina-Vene konflikti algust. Töö keskendus sellele, kuidas turud reageerivad välisšokkidele ning millist mõju avaldavad need sündmused küberturbe sektori aktsiatele, pakkudes seeläbi olulist ülevaadet ja väärtuslikku informatsiooni nii investoritele kui ka tööstusosapooltele.
Ebanormaalsete tootluste teoreetiline alus, millele töös keskenduti, toob esile konkreetsete sündmuste mõju aktsiatele ning uurib erinevaid meetodeid ebanormaalsete tootluste arvutamiseks. Positiivsete ja negatiivsete ebanormaalsete tootluste eristamine aitab mõista aktsiate käitumist väliste šokkide tingimustes ning annab investeerijatele vajalikke teadmisi turudünaamika mõistmiseks keerulistes oludes.

Töö analüüsis ka varasemaid uuringuid, mis käsitlesid väliste sündmuste mõju aktsiaturgudele, ning tõi välja erinevad arvutamismeetodid, nagu kumulatiivsed ebanormaalsed tootlused (CAR-id), keskmist kohandatud tootlusmudelid, kumulatiivsed keskmised ebanormaalsed tootlused (CAAR-id) ja keskmised ebanormaalsed tootlused (AAR-id). Need uuringud rõhutasid sündmuste-uuringute metoodika olulisust turu käitumise mõistmisel kriisitingimustes ning tõid esile erinevate sektorite reaktsioone välistele šokkidele.

Empiirilise analüüsi kaudu uuriti USA küberturbe ettevõtete ebanormaalseid tootlusi pärast COVID-19 pandeemia ja Ukraina-Vene konflikti algust. Sündmuste-uuringu metoodikat rakendati 20 USA küberturbe ettevõtte aktsiate ebanormaalsete tootluste hindamiseks võrreldes NASDAQi ja S&P500 indeksitega erinevatel ajavahemikel. Tulemused näitasid, et esimese kuu jooksul pärast mainitud sündmuste algust ei olnud aktsiate ebanormaalsed tootlused statistiliselt olulised, kuid päeva lähedal aset leidvate sündmuste puhul olid tootlused olulised, kinnitades uurimuse hüpoteese.

Autorite eeldused küberturbe ettevõtete suurenenud finantsjõudlusest ja nõudlusest pandeemia ajal said empiirilise kinnituse. Tulevased uuringud võiksid keskenduda pikemaajalistele analüüsidele, sektorite võrdlemisele ja Euroopa turu süvitsi uurimisele, integreerides kvalitatiivset informatsiooni. See aitaks mõista paremini küberturbe ettevõtete aktsiate käitumist keerulistes turutingimustes ning selgitada nende reageerimist erinevatele šokisündmustele, toetades investoreid muutlike turutingimuste navigeerimisel.

Non-exclusive licence to reproduce thesis and make thesis public

I, Yaroslav Nedvyga,

1. herewith grant the University of Tartu a free permit (non-exclusive licence) to

reproduce, for the purpose of preservation, including for adding to the DSpace digital archives until the expiry of the term of copyright,

"Abnormal returns of US cybersecurity stocks during COVID-19 pandemic and Russo-Ukrainian conflict"
supervised by
Junior Lecturer Mark Kantšukov.

2. I grant the University of Tartu a permit to make the work specified in p. 1 available to the public via the web environment of the University of Tartu, including via the DSpace digital archives, under the Creative Commons licence CC BY NC ND 3.0, which allows, by giving appropriate credit to the author, to reproduce, distribute the work and communicate it to the public, and prohibits the creation of derivative works and any commercial use of the work until the expiry of the term of copyright.

3. I am aware of the fact that the author retains the rights specified in p. 1 and 2.

4. I certify that granting the non-exclusive licence does not infringe other persons' intellectual property rights or rights arising from the personal data protection legislation.

Yaroslav Nedvyga
9/05/2024