ENTREPRENEURSHIP AND SUSTAINABILITY ISSUES
ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2023 Volume 11 Number 2 (December)
http://doi.org/10.9770/jesi.2023.11.2(31)

Publisher
http://jssidoi.org/esc/home

HYBRID THREATS AND THEIR IMPACT ON THE PERFORMANCE OF THE BUSINESS ENVIRONMENT*

Miroslava Barkóciová [1], Bohuslava Mihalčová [2], Filip Černák [3], Stanislav Šišulák [4]

[1,2] University of Economics in Bratislava, Faculty of Business Economics with seat in Košice, Department of Economics and Management, Tajovského 13, 040 01 Košice, Slovak Republic
[3] University of Prešov in Prešov, Faculty of Management and Business, Konštantínova 16, 080 01 Prešov, Slovak Republic
[4] Police Academy in Bratislava, Sklabinská 1, 835 17 Bratislava, Slovak Republic

E-mails: [1]miroslava.barkociova@euba.sk; [2]bohuslava.mihalcova@euba.sk; [3] fcernak@sitno.sk; [4] stanislav.sisulak@akademiapz.sk;

Received 8 September 2023; accepted 7 December 2023; published 30 December 2023

Abstract. The paper aims to assess the impact of hybrid threats on the performance of the business environment of the European Union countries. Hybrid threats were represented by six threats and their consequences, namely unavailability of ICT services due to hardware or software failure, unavailability of ICT services, unavailability of ICT services due to external attack, destruction or corruption of data due to malware infection or unauthorised intrusion, disclosure of confidential data due to intrusion, pharming, phishing attack or deliberate action of own employees, disclosure of confidential data due to negligent action of own employees. The performance of the business environment was assessed through the Country Competitiveness Index. The results showed that our selected threats and their consequences had a statistically significant impact on the performance of the business environment. We observed an adverse effect for unavailability of ICT services due to hardware or software failure, destruction, or corruption of data due to mal-ware infection or unauthorised intrusion, and disclosure of confidential data due to intrusion, pharming, phishing attack, or deliberate actions of own employees. Positive impacts on business environment performance were observed for unavailability of ICT services (insider attack), unavailability of ICT services due to external attacks and disclosure of confidential data due to negligent actions of own employees.

Keywords: business environment; cyber-attacks; cybersecurity; performance

Reference to this paper should be made as follows: Barkóciová, M., Mihalčová, B., Černák, F., Šišulák, S. 2023. Hybrid threats and their impact on the performance of the business environment. *Entrepreneurship and Sustainability Issues*, 11(2), 466-479. http://doi.org/10.9770/jesi.2023.11.2(31)

JEL Classifications: H55, O35, Z13

1. Introduction

In an era characterised by rapid technological advances and geopolitical complexity, the traditional boundaries that once defined security threats are blurred. The current global space creates possibilities for the emergence of the application of hybrid threats, a multifaceted and dynamic challenge that goes beyond the conventional categorisation of security risks. These hybrid threats represent a fusion of conventional, unconventional, and

* *The paper is part of the outputs of the project Research of educational concepts in the field of hybrid threats in selected EU countries with the subsequent development of the concept of education for the Slovak Republic project code in ITMS 2014+: 314011CDW7*

cyber threats, often organised by state and non-state actors, with the potential to disrupt national security and the stability and vitality of the global business environment.

This scientific article discusses the field of hybrid threats and their profound consequences for the performance of the business environment. The term "hybrid threats" encompasses various activities, from disinformation campaigns and cyber-attacks to economic coercion and proxy warfare. As these threats continue to evolve, their impact on businesses worldwide is becoming more significant.

This article aims to comprehensively examine the nature of hybrid threats, their modus operandi, and the complex web of connections between these threats and the business world. Through empirical research, implemented case studies and critical analysis, we clarify the multifaceted dimensions of this complex challenge and its consequences for businesses operating in a globalised economy.

The vulnerabilities to hybrid threats are exacerbated as the business environment becomes more interconnected and reliant on digital infrastructure. Companies are at risk of financial losses and face reputational damage, operational disruption, and regulatory scrutiny. Understanding the dynamics of hybrid threats is imperative for businesses to develop effective risk management strategies, enhance resilience, and ensure the continuity of operations in an increasingly uncertain world.

In our article, we will outline the various manifestations of hybrid threats, their effects on the economic and business environment, and the strategies organisations can use to mitigate these risks. We will contribute to the knowledge base that informs the decision-making processes of politicians, business leaders and security professionals in ensuring the integrity and performance of the modern business environment.

The use of information technology gives organisations a competitive advantage. Widespread access to the Internet has changed the way businesses manage their processes. With the rise of new devices, doing business has become easier. (Biclesanu et al. 2021) Information and technology services also pose a security risk to the enterprise in the form of leakage of sensitive information, unavailability of information and communication technologies, or data corruption due to attacks. Organisations, therefore, need to implement comprehensive security strategies to protect them from this risk. (Mosteanu, 2020; Ghelani, 2022; Gombár et al. 2022)

Many enterprises use antivirus software, firewalls, antispyware software, virtual private networks (VPNs), and the like to protect themselves from threats and secure their data. However, using these protections is often ineffective, hence the need for a comprehensive security strategy. (Mostenau, 2020) In addition to protection systems, the focus should be on detection systems that help gather information about threats and attacks. Detecting malicious actions is one of the most critical cybersecurity issues. Intrusion detection refers to the detection of specific patterns or observations of anomalies. Nowadays, it is necessary to pre-emptively anticipate incoming malicious activities so that we can react to them and prevent an attack in time before it causes any damage. (Pivarníková, Sokol, Bajtoš, 2020)

Early detection of security incidents and correct prediction of the evolution of an attack is the basis for an effective and timely response to cyber threats. The evolution of an attack depends on the next steps available to the attackers, their goals, and motivations. (Dovnikova et al., 2020; Vagaska et al. 2022)

While technology plays a critical role in addressing cybersecurity issues, the human aspects have recently gained serious attention. (David et al., 2020) Data loss or corruption can also occur in the event of intentional or unintentional actions by employees, hence the need to emphasise employee training in cybersecurity.

Human capital is considered the most essential resource in any organisation. However, most companies pay more attention to the external environment and pay little attention to their employees. Technological developments have changed our lives and habits. (Fernandes et al., 2023) Weritz (2022) emphasised in her work that organisations should monitor the skills of their employees and offer opportunities for individuals to develop their skills. She pointed out that entrepreneurial mindset, digital responsibility, digital literacy, transformational skills, personal development, communication, community management, data analytics, and web application development skills are critical in the digital workplace.

These threats are not only a danger to businesses themselves but equally dangerous to countries as well. A country needs consistent protection against these threats to avoid becoming unattractive to businesses, which will impact its business environment.

2. Business environment

The term business environment refers to all factors that impact business. This includes internal and external factors. Each of these factors somehow affects the business environment and the companies within it. Technological development has recently moved the business environment, its quality and development. The business environment, characterised by high instability and uncertainty, is much more precarious for enterprises because they need access to significant resources. Still, effective innovation depends, above all, on the quality and quantity of the resources that the enterprise controls. Managers are therefore called upon to consider innovation as a central factor in building the competitiveness and performance of their enterprises. They must, therefore, invest heavily in innovation, employee training and research and development. Otherwise, they are exposed to the destructive effects of a highly volatile environment, and their performance will decline as the business environment remains unstable. (Ruba et al., 2023; Mihalčová et al., 2021)

On the other hand, a healthy business environment can create a fairer market, facilitate flexibility in business operations and encourage technological innovation in enterprises. A good business environment has a more significant impact on large enterprises than on small enterprises. (Han et al., 2023; Straková et al., 2021)

The evolution of the business environment varies from country to country; therefore, the business environment gives some countries a competitive advantage. In their paper, Rusu and Dornean (2019) noted that a country must outperform its competitors in research and innovation, entrepreneurship, competition, and education. They investigated the impact of factors measuring the quality of entrepreneurial activities on national competitiveness in 28 European Union member states. Their research showed that innovation rate and job creation significantly influence the level of economic development of countries and their national competitiveness.

Technology has become an integral part of everyday and working life. However, with the development of information technology comes new risks, namely security risks. The business environment generates vast complex data that provides decision support through information processing and insight generation. (Lu, 2022) As most business processes and data-driven operations in today's business environment have moved into cyberspace, securing, protecting, and defending organisational information has become more critical. (Rawat et al., 2019)

According to Gamidullaeva & Gamagomedova (2023) and Šimberová et al. (2022), different business environments may have other impacts. Improvements in the institutional environment and greater certainty about the future significantly impact entrepreneurial activity and business performance.

In 2021, 22.2% of enterprises (with 10 or more employees and self-employed) in the EU corporate economy (excluding the mining and quarrying sector and the financial sector) experienced ICT security incidents resulting in different types of consequences, such as unavailability of ICT services, destruction or corruption of data, or disclosure of confidential data (Euostat, 2023).

Countries and supranational organisations such as the European Union are reshaping their traditional economic environments by promoting the use of broadband connectivity and the Internet, providing online services to citizens, facilitating investment in the spectrum of the digital economy, and introducing new business models suitable for the development of the digital economy. (Laitsou et al., 2020)

Eurostat (2023) also reported that, among EU countries, the highest proportion of enterprises that experienced ICT security incidents leading to unavailability of ICT services, destruction or corruption of data or disclosure of confidential data was in Finland, at more than two-fifths (43.8%), followed by the Netherlands and Poland (30.1% and 29.7%), the Czech Republic (29.3%) and Denmark (26.4%). At the other end of the scale, Bulgaria (11.0%), Portugal (11.5%), Slovakia (12.3%), Hungary (13.4%) and Cyprus (14.3%) had the lowest shares.

We see the impact of hybrid threats on the business environment in areas other than information. Examples include:

Economic impact - they create uncertainty and instability in a country, which can scare away foreign investors and cause a drop in economic confidence. This can harm business growth and investment.

Political destabilisation - creates political uncertainty and instability, which can result in changes in government policies, regulations, and legislation. This can affect businesses' strategic decisions and ability to plan long-term investments.

Information warfare - often involving disinformation campaigns and propaganda that can influence public opinion and perceptions of specific businesses and industries. Fake news can cause loss of customer and investor confidence. In a rapidly changing world, economies and companies must reshape their traditional models to adapt to a rapidly evolving digital environment. Information and communication technologies (ICT) have become more than a normal use. ICT has gradually become a critical operational component for individuals, businesses, and national economies. (Laitsou et al., 2020)

Social unrest - caused by hybrid threats can lead to riots and demonstrations that can disrupt normal business activities and even lead to loss of property and lives.

Corruption risk - in countries affected by hybrid threats, corruption and bribery may increase, resulting in an unsafe business environment for companies that seek to comply with ethical standards and legislation.

Therefore, businesses must be aware of hybrid threats and develop strategies to manage and protect against them. This may include improving cyber security, monitoring political and economic events, proactively managing risks, and working with local and international authorities to address these threats.

3. Hybrid threats

Hybrid threats represent one of the growing security challenges for the safe and effective management of critical infrastructure, digital systems and social domains worldwide. The deliberate misuse or disruption of these domains and digital technologies has widespread implications in various aspects of life, including daily activities, civil and military operations, transportation and aviation, communications, finance, and the interconnection of water, food and energy, medical treatments, and social media. (Vaseashta, 2022) Security is a serious issue that we all face. Every day, skilled hackers breach security and exploit vulnerabilities to gain access to top-secret and confidential data. (Fatima et al., 2023)

Vulnerabilities identified in Latin American countries include low cybersecurity awareness, lack of sufficiently implemented standards and regulations, use of updated software, security gaps in critical infrastructure, lack of training and specialisation, and the prevalence of advanced persistent threats (ATP). Investing and paying attention to cyber security in crucial public organisations and banking sectors is essential. (Flor-Unda et al., 2023)
One of the main aspects of hybrid threats to enterprises is cyber vulnerability. Cyber-attacks can cause service outages, steal sensitive data or damage confidential information assets. These attacks can be more complex and sophisticated, meaning businesses must invest in robust cyber security measures and keep up with the latest technology trends to protect their digital assets.

In addition, hybrid threats are often associated with manipulating public opinion and misinformation, which can affect business decisions and customer confidence. Businesses must also address the risk of economic destabilisation due to political conflicts and sanctions. It is crucial for businesses to be prepared for these hybrid threats and have rapid response and recovery strategies in place to minimise potential damage and maintain their resilience to these complex threats.

In their article, Mityakov et al. (2023) suggest 12 main "quick" indicators that can be used for operational monitoring of a country's economic security, grouped into four spheres. The choice of indicators was dictated by sufficient coverage of certain areas of economic security. In addition, the proposed indicators were used based on the availability of information from official sources and the required frequency of receiving information.

Another vital aspect of hybrid threats to businesses is their ability to interfere with global supply chains. In today's world, companies are often involved in large and complex chains involving suppliers and customers from different parts of the world. Hybrid threats such as trade blockades, cyber-attacks, or political manipulation can seriously affect these chains, with the potential to cause supply disruptions and increase logistics costs and business risks.

Therefore, businesses need to have comprehensive risk management and business continuity plans that consider hybrid threats. They need to actively monitor the geopolitical situation and cyber security trends to respond quickly to potential threats and minimise their impact. Collaboration with other businesses, government agencies, and security experts can also be critical to effectively defending against hybrid threats and maintaining stability in corporate operations.

Despite these risks, several strategies have emerged in the market that effectively combat hybrid threats. One of them is artificial intelligence, which helps improve the state of cybersecurity. (Rawal, 2022) In addition to protecting sensitive data and combating hybrid threats, these strategies help organisations prevent breaches and facilitate recovery and adaptation after such breaches. (Vaseashta, 2022)

There are several hybrid threat tools. Common ones encountered in practice are propaganda, disinformation, sabotage, economic warfare, or cyber-attacks. The sophistication of cyber-attack techniques poses a danger to businesses and can disrupt operations, destroy critical data, and damage reputations. The current wave of attacks surpasses and outpaces humans and even includes artificial intelligence (AI). (Guembe et al., 2022) Artificial intelligence, according to Rawal (2022), helps improve the state of cybersecurity. Still, on the other hand, cybercriminals are also using it to launch more targeted and sophisticated attacks.

Given the cyclical increase in security incidents, cybersecurity is a significant concern for all industries involved in digital activities. As more and more Internet of Things (IoT) devices are used in homes, offices, transport, healthcare and other locations, malicious attacks are becoming more frequent. Due to the vast amount of data IoT devices produce, Machine Learning (ML) is commonly used to detect attacks. (Prabakar et al., 2023)

Today's cyber-attacks on businesses have become an integral part of the digital age and pose a persistent threat to organisations of all sizes and sectors. One of the most common types of attack is ransomware, which encrypts an organisation's sensitive data and a subsequent ransom demand from the attackers. These attacks not only cause financial losses but also severely disrupt the operations and reputation of companies.

To prevent these attacks, businesses must strive to raise their employees' cyber security awareness and implement robust security measures, including firewalls, antivirus programs and network monitoring. In addition, it is essential to have a cyber-attack recovery plan in place to minimise losses and restore normal operations quickly. Cybersecurity has become a priority for businesses in today's digital era and requires constant investment and attention to protect against everchanging threats.

With the increasing severity and frequency of cyber-attacks, the rapid proliferation of smart objects is intensifying cybersecurity threats. Extensive data on communication traffic between Internet of Things (IoT) devices poses a significant challenge in protecting these devices from potential security breaches exacerbated by unbalanced network traffic data. Artificial intelligence technologies, particularly machine and deep learning, have shown promise in detecting and addressing these security threats targeting IoT networks. (Alkhudaydi et al., 2023)

Cyber-attack detection detects and responds to malicious or unauthorised activity on networks, computer systems and digital environments. The goal is to identify these attacks early, protect sensitive data and minimise potential damage. (Albakri et al., 2023)

Effective detection and prevention of cyber-attacks contribute to minimising economic losses, maintaining trust, promoting responsible digital transformation, ensuring supply chain resilience, and preventing potential damage. Detecting cyber-attacks involves proactive risk management, ethical responsibility, resilience and the well-being of individuals, organisations, and the planet. In addition, businesses prioritise long-term viability, and cyber-attack detection is essential in maintaining business continuity. By integrating robust cybersecurity practices into the fabric, society can move towards a safer, more secure, and responsible future. Organisations can avoid costly disruptions, financial losses and reputational damage by preventing and responding quickly to cyber threats. (Doynikova et al., 2020; Albakri et al., 2023)

As information technology has become an integral part of everyday as well as working life. They play a significant role in global communication. Tan et al. (2021) state that innovations and low cost in information technology have significantly increased the availability, use and performance of information technology.

According to Aghajani and Ghadimi (2018), most economic, business, cultural, and social interactions of countries at all levels, from individuals to NGOs and government institutions, occur in cyberspace. Moving these activities to cyberspace has brought with it several risks. A certain degree of instability, uncertainty or problems in this space can affect various aspects of life. (Li et al., 2020)

Duo et al. (2022) state that cyber-attacks can be divided into three classes: attacks on availability, integrity, and confidentiality. Availability attack is one of the most common cyber-attacks. It aims to block a communication network by making data and information inaccessible to the user. Typical availability attacks include DoS attacks, distributed DoS attacks and jamming attacks. An integrity attack is a compromise of integrity through falsifying data or control commands. There are many types of integrity attacks, e.g., false data injection, middlemen, sparse and replay attacks. Integrity attacks can occur in any part of the system because the attacker's target can be any system information. Attack methods include eavesdropping and a combination of DoS and integrity attacks.

Due to cyber-attacks, cybersecurity has become an essential part of any organisation's infrastructure. Cybersecurity involves practical measures to protect information, networks, and data from internal or external attacks. Cybersecurity experts safeguard networks, servers, intranets, and computer systems so that only authorised individuals can access this information (Jamal et al., 2021).

Safitra et al. (2023) describe in their work an evolutionary approach and its application to cyber-attack prevention through a methodological approach involving an evolutionary model. This model illustrates how modern cyber-physical systems can face attacks and evolve based on the experience of past security incidents. An evolutionary approach to cybersecurity thus allows organisations to evolve and adapt to new threats continuously, increasing their resilience to cyber-attacks. These efforts include developing the ability to anticipate threats, prepare responses to attacks, and quickly restore operations after incidents. In addition, an evolutionary approach enables organisations to improve their proactive cybersecurity capabilities continuously. This includes developing employee security training programs, raising security awareness throughout the organisation, and fostering a strong security culture. Therefore, an evolutionary approach helps organisations respond to cyberattacks but also helps prevent them from occurring in the first place.

Sensuse et al. (2022) recommend using big data, blockchain, biometrics, machine learning, cryptography, network security, artificial intelligence, and intrusion detection to achieve cybersecurity goals. Cybersecurity also needs risk assessment, management, and awareness so that the selected security technology can achieve the expected goals.

Cybersecurity solutions for information technology (IT) have been developed and refined for some time. The availability of sensitive data is highly valued, but in IT, the security of that data is of paramount importance. (Alzahrani & Aldhyan, 2023)

4. Methodology

In this paper, we focus on the impact of hybrid threats on the performance of the business environment in the European Union countries in 2022. The total sample consists of 26 countries belonging to the European Union. We excluded Malta from the assessment because no published data on the country's competitiveness existed. We determined the performance of the business environment based on the World Competitiveness Ranking (WCR) determined by IMD.

The World Competitiveness Ranking is based on 335 criteria selected based on comprehensive research. These criteria are regularly reviewed and updated in light of new research, data, and developments in the global economy. (IMD World Competitiveness Ranking, 2023) We consider WCR as a dependent variable in our study.

Six threats and consequences obtained from Eurostat databases represented hybrid threats as independent variables. We divided these threats into two groups, namely:

1. No harmful consequences.
2. With harmful consequences caused from inside or outside the company.

We included in the first group the unavailability of ICT services due to hardware or software failure, unavailability of ICT services (e.g., denial of service attacks, ransomware, hardware, or software failure).

The second group consists of the unavailability of ICT services due to an external attack (e.g., ransomware attacks, Denial of Service attacks), destruction or corruption of data due to malware infection or unauthorised intrusion, disclosure of confidential data due to intrusion, pharming, phishing attack or deliberate action by own employees, disclosure of confidential data due to inadvertent action by own employees.

We chose these factors based on data from Eurostat, which states that the most common consequence of security threats was the unavailability of ICT services due to hardware or software failure (18.7%). The unavailability of ICT services due to external attacks (e.g., ransomware attacks, denial of service attacks) was much less frequent (3.5%). EU businesses also reported data destruction or corruption caused by two types of incidents: hardware or software failure (3.9%) or malware infection or unauthorised intrusion (2.1%). The least frequent consequence of ICT security incidents was the disclosure of confidential data, which was related to two different reasons: intrusion, pharming, phishing attack, deliberate action by own employees (1.1%) and inadvertent action by own employees (1.0%) (Eurostat, 2023).

5. Results

At the beginning of the investigation, we assumed that hybrid threats represented by our selected variables negatively impact the performance of the business environment in the European Union countries.

The first step in analysing the data was to test what distribution it came from. Based on the Shapiro-Wilk test, we found that the data met the assumptions of a normal distribution.

Table 1. ANOVA regression

Model		Sum of Squares	df	Mean Square	F	Sig.
1	**Regression**	2675.721	6	445.953	3.002	.031[b]
	Residual	2822.819	19	148.569		
	Total	5498.540	25			

a. Dependent Variable: World Competitiveness Ranking
b. Predictors: (Constant), Disclosure of confidential data due to unintentional actions by own employees, Destruction or corruption of data due to infection of malicious software or unauthorised intrusion, Unavailability of ICT services due to hardware or software failures, Unavailability of ICT services due to attack from outside (e.g. Ransomware attacks, Denial of Service attacks), disclosure of confidential data due to intrusion, pharming, phishing attack, intentional actions by own employees, Unavailability of ICT services (e.g. Denial of Service attacks, ransomware attacks, hardware or software failures)

Source: own processing

The regression model presented in Table 1 shows statistical significance as the p-value (Sig.) is less than the set significance level of 0.05. This indicates that there is a statistically significant relationship between the dependent variable and the independent variables.

Table 2. Coefficients

Country	Non–malicious causes		Malicious causes caused by attack from inside or outside				World Competitiveness Ranking (Constant)	Ranking
	Unavailability of ICT services due to hardware or software failures	Unavailability of ICT services (e.g., Denial of Service attacks, ransomware attacks, hardware, or software failures)	Unavailability of ICT services due to attacks from outside (e.g., Ransomware attacks, Denial of Service attacks)	Destruction or corruption of data due to infection of malicious software or unauthorised intrusion	Disclosure of confidential data due to intrusion, pharming, phishing attacks, intentional actions by own employees	Disclosure of confidential data due to unintentional actions by own employees		
Austria	-0.79	1.01	0.02	-0.07	-0.07	0.07	46.18	8
Belgium	-1.33	1.60	0.03	-0.08	-0.15	0.19	45.87	9
Bulgaria	-0.55	0.65	0.01	-0.07	-0.09	0.05	29.49	26
Croatia	-0.84	1.00	0.01	-0.09	-0.19	0.20	32.91	21
Cyprus	-0.69	0.86	0.03	-0.13	-0.23	0.30	37.51	18
Czech Republic	-1.69	1.94	0.03	-0.14	-0.15	0.12	43.54	11
Denmark	-1.56	1.82	0.03	-0.07	-0.18	0.27	57.43	1
Estonia	-1.55	1.75	0.02	-0.07	-0.15	0.21	45.36	10
Finland	-2.66	2.99	0.03	-0.06	-0.21	0.37	53.43	4
France	-1.51	1.70	0.01	-0.06	-0.11	0.08	42.69	12
Germany	-1.58	1.81	0.02	-0.07	-0.11	0.15	49.20	7
Greece	-0.80	1.14	0.03	-0.06	-0.19	0.08	32.88	22
Hungary	-0.50	0.64	0.02	-0.07	-0.10	0.16	37.83	17
Ireland	-0.81	0.99	0.01	-0.02	-0.04	0.07	51.41	5
Italy	-0.88	1.06	0.02	-0.06	-0.06	0.06	37.34	19
Latvia	-1.03	1.17	0.02	-0.07	-0.19	0.21	38.14	14
Lithuania	-0.92	1.01	0.00	-0.07	-0.07	0.09	42.18	13
Luxembourg	-0.82	1.01	0.02	-0.10	-0.12	0.16	50.40	6
Netherlands	-1.63	2.00	0.04	-0.09	-0.30	0.29	54.15	3
Poland	-1.86	2.05	0.02	-0.11	-0.07	0.10	30.65	24
Portugal	-0.56	0.71	0.01	-0.08	-0.05	0.05	37.04	20
Romania	-1.13	1.27	0.02	-0.10	-0.07	0.08	30.55	25
Slovakia	-0.65	0.75	0.01	-0.04	-0.05	0.08	30.74	23
Slovenia	-0.78	0.90	0.01	-0.06	-0.15	0.08	37.88	16
Spain	-0.86	1.04	0.02	-0.10	-0.13	0.07	38.01	15
Sweden	-1.17	1.40	0.02	-0.07	-0.15	0.16	56.11	2

Dependent Variable: World Competitiveness Ranking

Source: own processing

Based on the analysis, we assessed the impact of our chosen independent variables (threats and consequences) on the dependent variable (competitiveness index) and then determined the ranking of the countries.

The analysis results showed that 3 out of the 6 selected threats and their consequences negatively impact the performance of the business environment in all countries. We consider the unavailability of ICT services due to hardware or software failure as a threat without harmful causes. However, we have seen the most significant negative impact on the business environment for this threat. The values ranged from -2.66 to -0.50. We also observed a negative effect when confidential data was disclosed because of employee intrusion, pharming, phishing attacks, or deliberate actions, where the values ranged from - 0.30 to - 0.04. The last threat with a negative impact was the destruction or corruption of data due to malware infection or unauthorised intrusion; for this threat, the values ranged from - 0.14 to - 0.02.

A surprising finding was that some of the threats and their consequences positively impacted the performance of the business environment. Specifically, these were unavailability of ICT services (e.g., Denial of Service attacks, ransomware, hardware, or software failure) (0.64 - 2.99), unavailability of ICT services due to external attack (e.g., ransomware, Denial of Service attacks) (0.00 - 0.04), and disclosure of confidential data due to inadvertent actions of own employees (0.05 - 0.37).

We hypothesise that the positive impact of these factors is due to increased attention from enterprises and security engineers. Enterprises and technicians try to prevent these threats by improving the security protocols used in enterprises.

Table 3. Cyber Safety

Ranking	Country	National Cyber Security Index (NCSI)	Global Cybersecurity Index (GCI)	Cybersecurity Exposure Index (CEI) 2020	Cyber-Safety Score (Mean Average of NCSI, GCI, and CEI)
1	Belgium	94.81	96.25	81.00	90.69
2	Finland	85.71	95.78	89.00	90.16
3	Spain	88.31	98.52	79.00	88.61
4	Denmark	84.42	92.60	88.30	88.44
5	Germany	90.91	97.41	75.90	88.07
6	Lithuania	93.51	97.93	70.30	87.25
7	France	84.42	97.60	77.20	86.41
8	Sweden	84.42	94.55	79.00	85.99
10	Portugal	89.61	97.32	69.70	85.54
11	Netherlands	83.12	97.05	73.80	84.66
12	Poland	87.01	93.86	71.40	84.09
13	Luxembourg	66.23	97.41	87.60	83.75
17	Croatia	83.12	92.53	74.50	83.38
18	Greece	96.10	93.98	60.00	83.36
19	Slovakia	83.12	92.36	73.80	83.09
20	Italy	79.22	96.13	73.10	82.82
26	Latvia	75.32	97.28	64.80	79.13
27	Ireland	75.32	85.86	74.50	78.56
28	Czech Republic	92.21	74.37	66.60	77.73
29	Hungary	67.53	91.28	71.40	76.74
33	Cyprus	66.23	88.82	66.60	73.88
35	Romania	89.61	76.29	53.80	73.23
40	Slovenia	59.74	74.93	71.70	68.79
51	Bulgaria	74.03	67.38	51.70	64.37

**Missing countries: Austria, Estonia, Malta*

Source: own processing

In addition to analysing the impact of the independent variables on the dependent variable, we have also reported the results of the cybersecurity scores of the European Union countries. SEON.IO compiled this global ranking by combining data from three central cybersecurity authorities, namely the National Cybersecurity Index (NCSI), the Global Cybersecurity Index (GCI) (2020) and the Cybersecurity Exposure Index (CEI) (2020) (SEON.IO, 2023).

From the above rankings, we have selected the countries of the European Union. The ranking of the countries corresponds to the ranking from the overall ranking. The index values and the overall scores of Austria, Estonia and Malta were not included in the given ranking; therefore, these countries are considered missing.

Table 4. Correlation

			World Competitiveness Ranking	Cyber-Safety Score (Mean Average of NCSI, GCI, and CEI)
Spearman's rho	World Competitiveness Ranking	Correlation Coefficient	1.000	0.540**
		Sig. (2-tailed)	.	0.006
		N	24	24
	Cyber-Safety Score (Mean Average of NCSI, GCI, and CEI)	Correlation Coefficient	0.540**	1.000
		Sig. (2-tailed)	0.006	.
		N	24	24

**. *Correlation is significant at the 0.01 level (2-tailed).*
Missing countries: Austria, Estonia, Malta

Source: own processing

In the end, we examined the relationship between a country's business environment's performance and cybersecurity. The correlation results indicate a moderate to moderately strong relationship between the variables. The value of the correlation coefficient between business environment performance represented by the variable global competitiveness ranking and cybersecurity represented by the variable cybersecurity score was equal to 0.540.

Conclusions

Examining hybrid threats and their impact on the business environment reveals a complex and evolving range of challenges and opportunities. As the global community grapples with the multifaceted nature of these threats, businesses are on the front lines of this fight and face significant risks and responsibilities.

Hybrid threats, combined with traditional and non-traditional elements, have demonstrated the ability to disrupt the digital realm and the physical and economic foundations of business. Many published case studies and analyses highlight the importance of recognising the interconnectedness of these threats and their potential to undermine corporate stability.

Faced with these challenges, businesses must adopt a proactive and multifaceted approach to risk management. This approach should include cyber defence and strategies to combat disinformation, manage economic pressures, and increase supply chain resilience. Cooperation between the public and private sectors is essential as it supports exchanging information on threats, the development of regulatory frameworks, and the implementing of best practices.

Furthermore, resilience is a crucial theme in mitigating the impact of hybrid threats on the business environment. Resilient organisations could adapt, recover, and continue operating despite negative influences from the external environment. By embedding resilience into corporate culture and strategies, businesses can increase their ability to withstand and recover from hybrid threats.

In conclusion, hybrid threats are a dynamic and ongoing challenge that requires vigilance, adaptability, and cooperation. As a vital part of modern society, the business environment must remain vigilant in identifying and mitigating these threats to ensure the stability and prosperity of global trade. As technological advances and geopolitical complexity continue, the study and understanding of hybrid threats will continue to evolve, and businesses must evolve with them to thrive in this everchanging environment. By comprehensively solving these threats and cooperating, we can work on a safer and more resilient business environment for the future.

The results of the analyses showed that our chosen independent variables have a statistically significant effect on the dependent variable. Thus, we can conclude that when the number of recorded threats and their consequences increases, changes in the business environment of a given country occur. We find that hybrid threats do not only affect the performance of a country's business environment in a negative sense, but some of them can also have a positive impact.

Ultimately, we compared the relationship between the performance of a country's business environment and cybersecurity. From this, we found that if a country has a better cybersecurity rating, the business environment performance scores higher and vice versa.

References

Aghajani, G., & Ghadimi, N. 2018. Multi-objective energy management in a microgrid. *Energy Reports*. 4, 218-225. https://doi.org/10.1016/j.egyr.2017.10.002

Albakri, A., Alabdullah, B., & Alhayan, F. 2023. Blockchain-Assisted Machine Learning with Hybrid Metaheuristics Empowered Cyber Attack Detection and Classification Model. *Sustainability*, 15. https://doi.org/10.3390/su151813887

Alkhudaydi, O.A., Krichen, M., & Alghamdi, A.D.A. 2023. Deep Learning Methodology for Predicting Cybersecurity Attacks on the Internet of Things. *Information*, 14. https://doi.org/10.3390/info14100550

Alzahrani, A., & Aldhyani, T.H.H. 2023. Design of Efficient Based Artificial Intelligence Approaches for Sustainable of Cyber Security in Smart Industrial Control System. *Sustainability*, 15. https://doi.org/10.3390/su15108076

Biclesanu, I., Anagnoste, S., Branga, O., & Savastano, M. 2021. Digital Entrepreneurship: Public Perception of Barriers, Drivers, and Future. *Administrative Sciences*, 11. https://doi.org/10.3390/admsci11040125

David, D.P., Keupp, M.M., & Mermoud, A. 2020. Knowledge absorption for cyber-security. *Computers in Human Behavior*, 106. https://doi.org/10.1016/j.chb.2020.106255

Doynikova, E., Novikova, E., & Kotenko, I. 2020. Attacker Behaviour Forecasting Using Methods of Intelligent Data Analysis: A Comparative Review and Prospects. *Information*, 11. https://doi.org/10.3390/info11030168

Duo, W., Zhou, M., & Abusorrah, A. 2022. Survey of Cyber Attacks on Cyber Physical Systems: Recent Advances and Challenges. *IEEE/CAA Journal of Automatica Sinica*, 9(5), 784-800. https://doi.org/10.1109/JAS.2022.105548

Eurostat. 22% of EU enterprises had ICT security incidents. [online]. 2023. 22% of EU enterprises had ICT security incidents - Products Eurostat News - Eurostat (europa.eu) Eurostat. Security incidents and consequences by size class of enterprise. [online]. 2022. Statistics | Eurostat (europa.eu).

Fatima, A. et al. 2023. Impact and Research Challenges of Penetrating Testing and Vulnerability Assessment on Network Threat. In: International Conference on Business Analytics for Technology and Security (ICBATS). Dubai. United Arab Emirates. 2023. pp. 1-8. ISBN 979-8-3503-3564-4. https://doi.org/10.1109/ICBATS57792.2023.10111168

Fernandes, R., Sousa, B.B., & Fonseca, M., & Oliveira, J. 2023 Assessing the Impacts of Internal Communication: Employer Branding and Human Resources. *Administrative Sciences*, 13. https://doi.org/10.3390/admsci13060155

Flor-Unda, O., Simbaña, F., Larriva-Novo, X., Acuña, Á., Tipán, R., & Acosta-Vargas, P. 2023. A Comprehensive Analysis of the Worst Cybersecurity Vulnerabilities in Latin America. *Informatics*, 10. https://doi.org/10.3390/informatics10030071

Gamidullaeva, L., & Agamagomedova, S. 2023. How Administrative Regulation Institutional Factors Affect the Business Efficiency in a Region: A Case Study of Russian Regions. *Economies*, 11. https://doi.org/10.3390/economies11030100

Ghelani, D. 2022. Cyber Security, Cyber Threats, Implications and Future Perspectives: A Review. *American Journal of Science, Engineering and Technology*, 3(6), 12-19.

Gombár, M., Korauš, A., Vagaská, A., & Tóth, Š. 2022. Analytical View on the Sustainable Development of Tax and Customs Administration in the Context of Selected Groups of the Population of the Slovak Republic. *Sustainability*, 14, 1891. https://doi.org/10.3390/su14031891

Guembe, B., Azeta, A, Misra, S., Osamor, V.C., Fernandez-Sanz, L., & Pospelova, V.. 2022. The Emerging Threat of Ai-driven Cyber Attacks: A Review. *Applied Artificial Intelligence*, 36(1). https://doi.org/10.1080/08839514.2022.2037254

Han, Y., Pan, Ch., & Jin, F. 2023. Does the Improvement of the Business Environment Improve the Innovation Efficiency of Enterprises? Evidence from the Listed Companies in China. *Sustainability*, 15. https://doi.org/10.3390/su151411424

IMD. World Competitiveness Ranking. [online]. 2022. World Competitiveness – IMD business school for management and leadership courses.

Jamal, A.A., et al. 2023. A review on security analysis of cyber physical systems using Machine learning. IMaterials Today: Proceedings, 80, 2302-2306. https://doi.org/10.1016/j.matpr.2021.06.320

Laitsou, E., Kargas, A., & Varoutas, D. 2020. Digital Competitiveness in the European Union Era: The Greek Case. *Economies*, 8. https://doi.org/10.3390/economies8040085

Li, N., Tsigkanos, Ch., Jin, Z., Hu, Z., & Ghezzi, C. 2020. Early validation of cyber–physical space systems via multiconcerns integration. *Journal of Systems and Software*, 170. https://doi.org/10.1016/j.jss.2020.110742

Lu, J. 2022. Data science in the business environment: Insight management for an Executive MBA. *The International Journal of Management Education*, 20(1). https://doi.org/10.1016/j.ijme.2021.100588

Mihalčová, B., Korauš, A., Prokopenko, O., Hvastová, J., Freňáková, M., Gallo, P., & Beáta, B. 2021. Effective Management Tools for Solving the Problem of Poverty in Relation to Food Waste in Context of Integrated Management of Energy. *Energies*, 14, 4245. https://doi.org/10.3390/en14144245

Mityakov, S.N., Mityakov, E.S., Ladynin, A.I., Nazarova, E.A. 2023. Country Economic Security Monitoring Rapid Indicators System. *Economies*, 11. https://doi.org/10.3390/economies11080208

Mosteanu, N.R. 2020. Artificial Intelligence and Cyber Security – Face to Face with Cyber Attack – a Maltese Case of Risk Management Approach. *Ecoforum Journal*, 9(2).

Perera, S., Jin, X., Maurushat, A. 2022. Opoku De-Graft Joe. Factors Affecting Reputational Damage to Organisations Due to Cyberattacks. *Informatics*, 9 https://doi.org/10.3390/informatics9010028

Pivarnikova, M., Sokol, P., Bajtos, T. 2020. Early-Stage Detection of Cyber Attacks. *Information*, 11. https://doi.org/10.3390/info11120560

Prabakar, D., Sundarrajan, M., Manikandan, R., Jhanjhi, Z.N., Masud, M., & Alqhatani, A. 2023. Energy Analysis-Based Cyber Attack Detection by IoT with Artificial Intelligence in a Sustainable Smart City. *Sustainability*, 15. https://doi.org/10.3390/su15076031

Rawal, B.S., Patel, S., Sathiyanarayanan, M. 2022. Identifying DDoS Attack using Split-Machine Learning System in 5G and Beyond Networks. In: IEEE INFOCOM 2022 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS). New York. USA. 2022. pp. 1-6. https://doi.org/10.1109/INFOCOMWKSHPS54753.2022.9798301

Rawat, D.B., Doku, R., Garuba, M. 2021. Cybersecurity in Big Data Era: From Securing Big Data to Data-Driven Security. In: IEEE Transactions on Services Computing. 14(6), 2055-2072. https://doi.org/10.1109/TSC.2019.2907247

Ruba, R.M., Chiloane-Tsoka, G.E., & Van der Westhuizen, T. 2023. Moderating Effect of Business Environmental Dynamism in the Innovtivness—Company Performance Relationship of Congolese Manufacturing Companies. *Economies*, 11. https://doi.org/10.3390/economies11070191

Rusu, V. D., & Dornean, A. 2019. The Quality of Entrepreneurial Activity and Economic Competitiveness in European Union Countries: A Panel Data Approach. *Administrative Sciences*, 9. https://doi.org/10.3390/admsci9020035

Safitra, M. F., Lubis, M., & Fakhrurroja, H. 2023. Counterattacking Cyber Threats: A Framework for the Future of Cybersecurity. *Sustainability*, 15. https://doi.org/10.3390/su151813369

Sensuse, D.I, Putro, P.A.W., Rachmawati, R., & Sunindyo, W. D. 2022. Initial Cybersecurity Framework in the New Capital City of Indonesia: Factors, Objectives, and Technology. *Information*, 13. https://doi.org/10.3390/info13120580

SEON.IO. Global Cybercrime Report: Which Countries Are Most at Risk in 2023. [online]. 2023. Global Cybercrime Report: Countries Most at Risk in 2023 | SEON.

Straková, J., Korauš, A., Váchal, J., Pollák, F., Černák, F., Talíř, M., & Kollmann, J. Sustainable Development Economics of Enterprises in the Services Sector Based on Effective Management of Value Streams. *Sustainability*, 13, 8978. https://doi.org/10.3390/su13168978

Šimberová, I., Korauš, A., Schüller, D., Smolíkova, L., Straková, J., & Váchal, J. 2022. Threats and Opportunities in Digital Transformation in SMEs from the Perspective of Sustainability: A Case Study in the Czech Republic. *Sustainability*, 14, 3628. https://doi.org/10.3390/su14063628

Tan, S., Xie, P., Guerrero, J.M., Vasquez, J.C., Li, Y., & Guo, X. 2021. Attack detection design for dc microgrid using eigenvalue assignment approach. *Energy Reports*, 7(1), 469-476. https://doi.org/10.1016/j.egyr.2021.01.045

Vagaská, A., Gombár, M., & Korauš, A. 2022. Mathematical Modeling and Nonlinear Optimisation in Determining the Minimum Risk of Legalisation of Income from Criminal Activities in the Context of EU Member Countries. *Mathematics*, 10, 4681. https://doi.org/10.3390/math10244681

Vaseashta, A. 2022. Applying Resilience to Hybrid Threats in Infrastructure, Digital, and Social Domains Using Multisectoral, Multidisciplinary, and Whole-of-Government Approach. *Building Cyber Resilience against Hybrid Threats*, 42-59. https://doi.org/10.3233/NICSP61

Weritz, P., & Hey, L 2022. It's Time to Train the Workforce: Critical Skills in the Digital Workplace. *Administrative Sciences*, 12. https://doi.org/10.3390/admsci12030094

Funding: The paper is part of the outputs of the project Research of educational concepts in the field of hybrid threats in selected EU countries with the subsequent development of the concept of education for the Slovak Republic project code in ITMS 2014+: 314011CDW7.

Author Contributions: The authors contributed equally. All authors have read and agreed to the published version of the manuscript.

Ing. Miroslava BARKÓCIOVÁ, Economics and Management, Faculty of Business Economy, University of Economics in Bratislava, 040 01 Košice, Slovak Republic.
ORCID ID: https://orcid.org/0009-0006-7779-9043

prof. Ing. Bohuslava MIHALČOVÁ, PhD. & PhD. EUR ING, Economics and Management, Faculty of Business Economy, University of Economics in Bratislava, 040 01 Košice, Slovak Republic.
ORCID ID: https://orcid.org/0000-0001-7958-3429

Mgr. Filip ČERNÁK, is the Ph.D. Candidate at the Faculty of Management at the University of Prešov in Prešov, Slovak Republic.
ORCID ID: https://orcid.org/0000-0001-7812-9371

Assoc. Prof. Ing. Stanislav ŠIŠULÁK, PhD., MBA, Academy of the Police Force in Bratislava, Sklabinská 1, 835 17 Bratislava, Slovak Republic.
ORCID ID: https://orcid.org/0000-0003-4727-9582.