Uluslararası İleri Doğa Bilimleri ve Mühendislik Araştırmaları Dergisi
Sayı 8, S. 391-397, 9, 2024
© Telif hakkı IJANSER'e aittir
Araştırma Makalesi

IJANSER

https://as-proceeding.com/index.php/ijanser
ISSN:2980-0811

International Journal of Advanced Natural Sciences and Engineering Researches
Volume 8, pp. 391-397, 9, 2024
Copyright © 2024 IJANSER
Research Article

Cyber Security and Bomb Threats in Schools: A Case Study of Slovakia

František Vráb *

[1]*Department of Economics and Management/Faculty of Business Economics, University of Economics in Bratislava, Slovakia*

*(frantisek.vrab@euba.sk) *Email of the corresponding author*

(Received: 23 October 2024, Accepted: 27 October 2024)

(4th International Conference on Engineering, Natural and Social Sciences ICENSOS 2024, 22-23 October 2024)

ATIF/REFERENCE: Vráb, F. (2024). Cyber Security and Bomb Threats in Schools: A Case Study of Slovakia, *International Journal of Advanced Natural Sciences and Engineering Researches*, 8(9), 391-397.

Abstract – With the increasing number of bomb threats around the world, which are often part of hybrid attacks combining conventional tactics with cyber and information warfare, security is becoming an increasingly urgent issue. Slovakia has seen an increase in such threats, especially in schools. This article analyzes the nature of these threats, focusing on attacker tactics and motivations. It also examines the preparedness and reactions of the Slovak security forces based on an extensive research study. This study focuses on the perception of cyber security risks among university students in order to gain knowledge relevant to security in schools. The research revealed a high level of risk perception in the area of cyber espionage, disruption of IT infrastructure, hostile campaigns and cyber terrorism. These findings highlight the importance of education and robust security measures in schools. The article concludes by emphasizing a comprehensive security approach that integrates physical security measures with robust cyber security protocols and a culture of vigilance.

Keywords – Bomb Threats, Hybrid Threats, Cyber-Attacks, Disinformation, Schools, Security, Prevention.

I. INTRODUCTION

This article examines the rising threat of bomb threats in schools, particularly in Slovakia, emphasizing the need to address these threats in conjunction with cybersecurity. It explores the evolving nature of cyber threats and their connection to physical attacks, advocating for a comprehensive security approach that integrates physical security measures with robust cybersecurity protocols. The research also delves into university students' perceptions of cyber security risks to identify vulnerabilities and propose preventive measures.

II. MATERIALS AND METHOD

Historical analyses of school bombings reveal a troubling trend: the increasing use of hybrid tactics in which cyberattacks are used to amplify fear, disrupt response efforts, and amplify the effects of physical attacks [11]. This chapter explores this link, drawing on historical examples and current cyber security research to highlight the key role of cyber security in mitigating the threat of bomb attacks in educational environments. As outlined in the previous section, school bombings have occurred with devastating regularity throughout history. Although the motivations differ, these attacks share common features:

- **Targeting vulnerability:** Schools symbolize innocence and learning, making them attractive targets for those seeking to inflict maximum psychological and social harm.

- **Devastating impact:** These attacks result in tragic loss of life, especially among children, with long-term consequences for survivors and communities.
- **Evolving Tactics:** Hybrid attack strategies are increasingly integrating bomb threats, which are combined with cyber-attacks and disinformation campaigns to maximize disruption and sow chaos.

Cybersecurity is no longer a peripheral concern but a central component of comprehensive school safety strategies. It plays a critical role in preventing and mitigating bomb attacks in multiple ways:

- **Threat detection and disruption:** Robust cybersecurity systems can help identify online communication patterns and activities that may signal planned attacks, enabling proactive intervention.
- **Information Protection:** Securing sensitive school data, including building plans, security protocols and emergency response procedures, prevents attackers from using this information to facilitate physical attacks.
- **Communication and Coordination:** Secure communication channels are essential for an effective emergency response during and after an attack, ensuring a reliable flow of information between school officials, law enforcement and first responders.
- **Resilience and recovery:** Cyber security measures can help schools recover critical systems and data after an attack, minimizing disruption to learning activities and facilitating a return to normalcy.

The research presented in this chapter is focused on the perception of cyber security risks among university students, offering valuable knowledge applicable to school security. Understanding how individuals perceive and respond to cyber threats can help develop tailored training programs and awareness campaigns for students, teachers, and administrators. Key areas include:

- **Cultivating Cyber Hygiene:** Educating school communities about online security best practices, such as strong password management, phishing awareness, and responsible social media use, can reduce vulnerabilities exploited by attackers.
- **Elevating Threat Awareness:** Increasing awareness of the potential for hybrid attacks, where cyberattacks are used in conjunction with physical threats, can help schools prepare for a broader spectrum of scenarios.
- **Fostering a Culture of Vigilance:** Encouraging students and staff to report suspicious online activity or concerning behavior can contribute to early threat detection and prevention.

The history of school bombings demonstrates the urgent need for comprehensive security measures that integrate physical and cyber security strategies. By understanding the evolving nature of threats and leveraging cybersecurity research, schools can improve their preparedness, strengthen their resilience, and create a safer learning environment for all.

Data Collection and Instrument Development

A multi-phase methodology was used to assess cyber security risk perception [1]. Initially, key constructs related to cybersecurity threats were identified through a comprehensive review of relevant literature and consultation with 15 subject matter experts specializing in mathematical modeling, hybrid threats, and psychology. Based on these constructs, a 39-item questionnaire using a 5-point Likert scale for responses was developed. Each item addressed a specific aspect of cybersecurity risk, categorized into five distinct pillars:

1. Cyber espionage (CYBSPY)
2. Disruption or reduction of IT infrastructure resilience (DISRIT)
3. Hostile campaigns (ENECAM)
4. Violation or reduction of the security of electronic public administration (DISREG)
5. Cyber terrorism (CYBTER)

Prior to full data collection, it was tested to ensure clarity, comprehensibility and consistency. The reliability of the instrument was assessed using Cronbach's alpha of 0.95047, indicating a high degree of internal consistency.

Sample and data collection:

The research sample consisted of 964 university students from Slovakia (60.166%) and the Czech Republic (39.834%). The sample consisted of 54.046% male and 45.954% female students with an average age of 26.03±0.51 years. The participants were enrolled in bachelor's, master's and doctoral programs in various fields. Data collection took place online using Google Forms from February 2023 to July 2023.

Factor model development and confirmatory factor analysis:

To analyze the basic structure of cyber security risk perception, a theoretical factor model (FMCS) was developed, which assumes that 39 observed variables (items in the questionnaire) are indicators of five latent constructs (pillars of cyber security). Confirmatory factor analysis (CFA), a structural equation modeling (SEM) technique, was used to test the hypothesized model. CFA allows assessment of model fit by evaluating relationships between observed indicators and latent constructs.

Model fit index:

Several fit indices were used to evaluate the congruence between the theoretical model and the observed data. These included:

- $\chi 2$/df: Chi-square statistic in relation to degrees of freedom.
- RMSEA: Root Mean Squared Error of Approximation.
- TLI: Tucker-Lewis index.
- CFI: Comparative Fit Index.
- SRMR: Standardized Root Residue.

Optimal values for these indices indicate a good fit between the model and the data, indicating that the model adequately accounts for the observed relationships between the variables.

Data analysis:

CFA was conducted using specialized SEM software to estimate model parameters and assess model fit. The statistical significance of model coefficients was evaluated to determine the strength and direction of relationships between latent constructs and their corresponding indicators. The aim of the analysis was to answer the following research questions:

- What is the relationship between the defined pillars of cyber security and the demographic indicators of the research sample?
- Are there differences in the perception of cyber threats between Slovak and Czech students?

The aim of the study was to provide a comprehensive and scientifically based analysis of cyber risk perception among university students in Slovakia and the Czech Republic.

III. RESULTS

This section presents the results of the statistical analysis conducted on the data collected from the cybersecurity risk perception questionnaire. The analysis focuses on understanding how different factors contribute to the overall perception of cybersecurity threats.

Analysis of the 5-Factor Model of Cybersecurity:

The Confirmatory Factor Analysis (CFA) of the 5-factor model of cybersecurity for the entire research set (N=964) reveals that all items in the research instrument significantly influence the defined pillars of cybersecurity ($p<0.05$). A detailed analysis of each cybersecurity pillar is provided below.

Cyber Spying (CYBSPY)

The first pillar, cyber spying (CYBSPY), comprises nine items (CSPYQ1 to CSPYQ9). The item with the lowest perceived risk (low risk) is CSPYQ3, with a standardized regression weight of 0.295 ($p<0.001$). This suggests that respondents do not consider outsourcing cybersecurity solutions to be a significant risk in the context of cyber spying. Conversely, the item with the highest perceived risk is CSPYQ5 (inappropriately set and applied cybersecurity policies), with a standardized regression weight of 0.658

(p<0.001). This is followed by CSPYQ8 (purchase of ICT through unverified intermediaries without knowledge of the product chain) with a weight of 0.650 (p<0.001), and CSPYQ7 (insufficient training of employees in cybersecurity) with a weight of 0.643 (p<0.001). Other items with a high level of risk perception (standardized regression weight > 0.600) include CSPYQ4 (cybersecurity not addressed comprehensively), CSPYQ1 (insufficient allocation of funds to cybersecurity), and CSPYQ6 (insufficient vetting of employees). Respondents assigned a medium level of risk to CSPYQ9 (sensitive information at risk due to the use of personal devices) and CSPYQ2 (ICT manufacturers and suppliers with ties to foreign governments).

Disrupting or Reducing IT Infrastructure Resilience (DISRIT)

The second pillar, disrupting or reducing IT infrastructure resilience (DISRIT), consists of 12 items (DRITQ1-DRITQ12). Nine of these items were assigned a high level of risk (standardized regression weight > 0.600). The item with the highest perceived risk is DRITQ10 (fragmentation of communication systems in public administration), with a standardized regression weight of 0.679 (p<0.001). This is followed by DRITQ1 (risk of attacks on critical information infrastructure) with a weight of 0.669 (p<0.001), and DRITQ2 (insufficient funds for cybersecurity courses and expert hiring) with a weight of 0.661 (p<0.001). Other high-risk items include DRITQ11 (lack of central methodologies for computing equipment use), DRITQ5 (security testing not systematically carried out), DRITQ3 (strategic industries not included in critical infrastructure), DRITQ12 (lack of mandatory email encryption), DRITQ7 (incorrect prioritization of cybersecurity investments), and DRITQ8 (insufficient cybercrime legislation). Items with a medium level of risk include DRITQ9 (use of outdated information infrastructure systems), DRITQ4 (public administration employees lacking cybersecurity awareness), and DRITQ6 (attacks through supply chains).

Enemy Campaigns (ENECAM)

The third pillar, enemy campaigns (ENECAM), comprises five items (ECQ1-ECQ5). The item with the highest perceived risk is ECQ3 (ownership structure of internet media with the potential for manipulation), with a standardized regression weight of 0.677 (p<0.001). This is followed by ECQ4 (insufficient vetting of public administration employees) with a weight of 0.641 (p<0.001), and ECQ1 (potential for social unrest due to hostile campaigns) with a weight of 0.622 (p<0.001). Items with a medium level of risk include ECQ5 (legislation on information access potentially endangering cybersecurity) and ECQ2 (use of social networks for disinformation campaigns).

Disrupting or Reducing eGovernment Security (DISREG)

The fourth pillar, disrupting or reducing eGovernment security (DISREG), consists of six items (GREGQ1-GREGQ6). The majority of these items have a standardized regression weight greater than 0.700, indicating a high level of perceived risk. The item with the highest perceived risk is GREGQ3 (insufficient security of government information systems) with a standardized regression weight of 0.741 (p<0.001). This is followed by GREGQ4 (poor cybersecurity policy setting) with a weight of 0.721 (p<0.001), GREGQ5 (insufficient cybersecurity education for government employees) with a weight of 0.716 (p<0.001), and GREGQ2 (underestimation of cyber threats in public administration) with a weight of 0.707 (p<0.001). Other high-risk items include GREGQ1 (insufficient funding for cybersecurity) and GREGQ6 (low level of public awareness about cybersecurity).

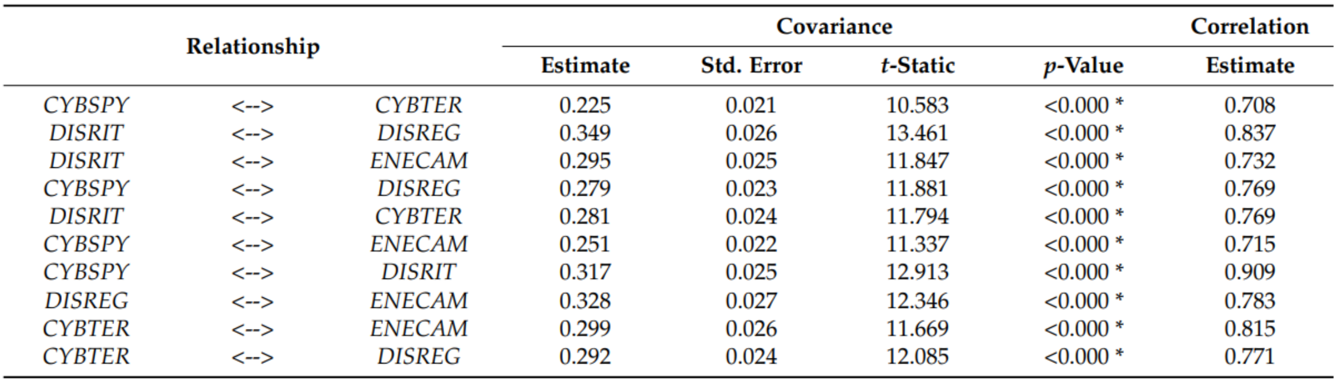
Cyberterrorism (CYBTER)

The fifth and final pillar, cyberterrorism (CYBTER), consists of seven items (CTQ1-CTQ7). The item with the highest perceived risk is CTQ6 (management of sympathizers by third parties for terrorist purposes), with a standardized regression weight of 0.730 (p<0.001). This is followed by CTQ4 (obtaining sensitive information for use in a kinetic attack) with a weight of 0.705 (p<0.001). Other high-risk items include CTQ5 (spreading radicalization propaganda) and CTQ7 (low preparedness of security forces for digital environments). Items with a medium level of risk include CTQ3 (energy blackouts), CTQ1 (blackmail and intimidation), and CTQ2 (destruction of technology).

Relationships Between Cybersecurity Pillars:

An analysis of the relationships between the defined pillars of cybersecurity is presented in Table 1. All links are statistically significant (p<0.05). The strongest correlation is observed between cyber spying (CYBSPY) and disrupting or reducing IT infrastructure resilience (DISRIT) with a correlation coefficient of 0.909 (p<0.001). Other significant relationships include DISRIT and DISREG (0.837, p<0.001), and CYBTER and ENECAM (0.815, p<0.001). The weakest correlation is between CYBSPY and CYBTER (0.708, p<0.001). In terms of overall importance, respondents ranked the pillars as follows: DISRIT (22.284%), DISREG (21.842%), ENECAM (19.532%), CYBTER (18.381%), and CYBSPY (17.961%). This indicates a relatively balanced perception of risk across all pillars. Results should be clear and concise. The most important features and trends in the results should be described but should not be interpreted in detail.

Table 1. Cybersecurity Pillar Correlations (N = 964)



Relationship			Covariance				Correlation
			Estimate	Std. Error	*t*-Static	*p*-Value	Estimate
CYBSPY	<-->	*CYBTER*	0.225	0.021	10.583	<0.000 *	0.708
DISRIT	<-->	*DISREG*	0.349	0.026	13.461	<0.000 *	0.837
DISRIT	<-->	*ENECAM*	0.295	0.025	11.847	<0.000 *	0.732
CYBSPY	<-->	*DISREG*	0.279	0.023	11.881	<0.000 *	0.769
DISRIT	<-->	*CYBTER*	0.281	0.024	11.794	<0.000 *	0.769
CYBSPY	<-->	*ENECAM*	0.251	0.022	11.337	<0.000 *	0.715
CYBSPY	<-->	*DISRIT*	0.317	0.025	12.913	<0.000 *	0.909
DISREG	<-->	*ENECAM*	0.328	0.027	12.346	<0.000 *	0.783
CYBTER	<-->	*ENECAM*	0.299	0.026	11.669	<0.000 *	0.815
CYBTER	<-->	*DISREG*	0.292	0.024	12.085	<0.000 *	0.771

Bomb Threats in Slovakia: A Geographic and Statistical Overview

On May 13, 2024, 1,323 bomb threats against schools were reported throughout Slovakia [8]. Figure 1 graphically shows the distribution of these threats by region.

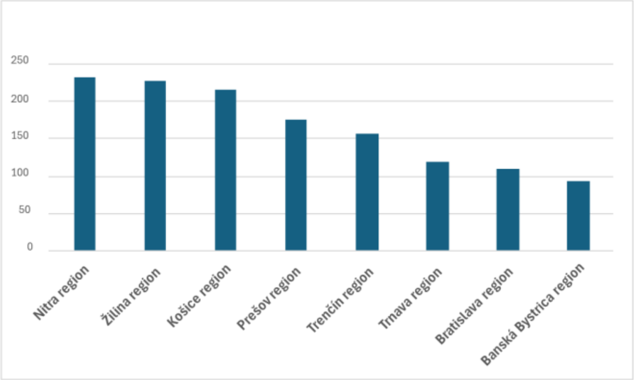


Fig. 1 Bomb threats in Slovakia

As depicted in figure 1, the Nitra, Žilina, and Košice regions were the most affected. These incidents underscore the vulnerability of schools to hybrid threats, which combine traditional methods with cyberattacks and disinformation campaigns. The results of the cybersecurity risk perception questionnaire provide valuable insights for enhancing school safety in the context of bomb threats [11]. The analysis revealed several key findings:

- **High-risk perception:** Respondents assigned a high level of risk to various cybersecurity threats, including cyber spying, disruption of IT infrastructure, enemy campaigns, and cyberterrorism. This indicates a heightened awareness of the potential consequences of cyberattacks, including their role in facilitating physical attacks like bombings.
- **Interconnectedness of threats:** The strong correlation between different cybersecurity pillars (e.g., cyber spying and IT infrastructure disruption) emphasizes the interconnected nature of these

threats. This highlights the need for a holistic approach to cybersecurity, where vulnerabilities in one area can have cascading effects on others.

- **Importance of education and awareness:** The findings underscore the importance of cybersecurity education and awareness programs for students, teachers, and administrators. By promoting cyber hygiene, enhancing threat awareness, and fostering a culture of vigilance, schools can strengthen their defenses against cyberattacks that may precede or accompany bomb threats.
- **Need for robust security measures:** The perceived high risk of cyber threats reinforces the necessity for schools to implement robust cybersecurity measures. This includes securing sensitive data, implementing strong authentication protocols, and regularly testing and updating security systems.

Connecting Cybersecurity and Bomb Threat Prevention:

The results of the cybersecurity risk perception questionnaire provide valuable insights for enhancing school safety in the context of bomb threats. The analysis revealed several key findings:

- **High-risk perception:** Respondents assigned a high level of risk to various cybersecurity threats, including cyber spying, disruption of IT infrastructure, enemy campaigns, and cyberterrorism. This indicates a heightened awareness of the potential consequences of cyberattacks, including their role in facilitating physical attacks like bombings.
- **Interconnectedness of threats:** The strong correlation between different cybersecurity pillars (e.g., cyber spying and IT infrastructure disruption) emphasizes the interconnected nature of these threats. This highlights the need for a holistic approach to cybersecurity, where vulnerabilities in one area can have cascading effects on others.

- **Importance of education and awareness:** The findings underscore the importance of cybersecurity education and awareness programs for students, teachers, and administrators. By promoting cyber hygiene, enhancing threat awareness, and fostering a culture of vigilance, schools can strengthen their defences against cyberattacks that may precede or accompany bomb threats.
- **Need for robust security measures:** The perceived high risk of cyber threats reinforces the necessity for schools to implement robust cybersecurity measures. This includes securing sensitive data, implementing strong authentication protocols, and regularly testing and updating security systems.

Recommendations for Improved Security:

- **Cybersecurity integration:** Schools should integrate cybersecurity considerations into their overall security planning and risk assessments. This includes recognizing the potential for cyberattacks to facilitate or amplify the impact of bomb threats.
- **Information sharing:** Establish channels for secure information sharing between schools, law enforcement, and cybersecurity agencies to facilitate threat detection and coordinated response efforts.
- **Cybersecurity training:** Provide comprehensive cybersecurity training for students, teachers, and staff, focusing on threat awareness, online safety practices, and incident reporting procedures.
- **Investment in technology:** Invest in robust cybersecurity technologies and infrastructure to protect school networks, data, and communication systems from unauthorized access and disruption.

By connecting the analysis of bomb threats with the findings of the cybersecurity risk perception questionnaire, this chapter emphasizes the crucial role of cybersecurity in preventing and mitigating these threats. By adopting a comprehensive approach that integrates physical security measures with robust cybersecurity protocols and a culture of vigilance, schools can create safer learning environments for all.

IV. DISCUSSION

This study analyzes the differences in perception of cybersecurity risks among university students in Slovakia and the Czech Republic. The research focuses on five key areas of cybersecurity: cyber espionage, disruption of IT infrastructure, hostile campaigns, disruption of eGovernment security, and cyberterrorism. The findings indicate that Slovak students generally perceive a higher level of risk across all areas compared to Czech students. This difference in risk perception highlights the need for tailored cybersecurity education and awareness programs in both countries. The study emphasizes the importance of preparedness and a comprehensive approach to cybersecurity in the face of evolving hybrid threats.

V. CONCLUSION

This research highlights the blurring of lines between physical and cyber threats, particularly in the context of bomb attacks. The study, focusing on university students, provides insights into the varying perceptions of cyber threats among different groups. It underscores the necessity for tailored security strategies and proposes recommendations for enhancing school safety through measures like multi-factor authentication, cybersecurity training, and robust emergency response plans. A holistic approach integrating physical and cyber security measures is crucial to create a safer learning environment.

ACKNOWLEDGMENT

The author expresses his sincere thanks to the company Training & Consulting, s.r.o., for its invaluable contribution to this research effort. Their unwavering commitment to solving complex organizational challenges, together with their generous support, insight and expertise, were key to the successful completion of this study. We also thank the cyber security community, which is taken care of by the National Coordination Center of the Slovak Republic (NCC-SK). Their commitment to enhancing national cybersecurity capabilities and fostering collaboration has created a supportive environment for research and innovation in this critical area.

REFERENCES

[1] Anderson, F. Crucible of War: The Seven Years' War and the Fate of Empire in British North America, 1754-1766. New York: Alfred A. Knopf, 2000.

[2] Bartoš, Alexander. 2022. The fog of hybrid warfare. Another view of the conflicts of the 21st century.2022. Torden.

[3] Bjorge, G. J. "Compound Warfare in the Military Thought and Practice of Mao Zedong and the Chinese People's Liberation Army's Huai Hai Campaign (November 1948 – January 1949)," in Compound Warfare: That Fatal Knot, ed. Thomas M. Huber (Leavenworth, KS, 2002), pp. 169–219.

[4] Clausewitz, C von, 1780-1831; Howard, M E, 1922-; PARET, P, On war 1976

[5] Gombár, M. Vagaská, A. Korauš A. Račková, P. Pavlína. Application of Structural Equation Modelling to Cybersecurity Risk Analysis in the Era of Industry 4.0. Journal of Cybersecurity, 2023, roč. 5, č. 2, s. 120-135.

[6] Hoffman, F. G. 2007. Conflict in the 21st Century: The Rise of Hybrid Wars. In Potomac Institute for Policy Studies, 2007.

[7] Merriam-Webster. 1996. Hybrid. https://www.merriam-webster.com/dictionary/hybrid

[8] Ministry of the Interior of the Slovak Republic. 2024.Press release on bomb threats. https://tinyurl.com/y2tmweny

[9] Moltke, Helmuth Graf von. 1995. Moltke on the Art of War: Selected Writings. New York: Presidio Press, ISBN 0-89141-575-0.

[10] Strassler, R. B., 1937-; Crawley, R, The landmark Thucydides : a comprehensive guide to the Peloponnesian War Thucydides; 1840-1893

[11] Vráb, František. 2023. A model for the prevention of hybrid threats in the enterprise environment. In: MTP no. 2, s. 32-38. https://tinyurl.com/3vv27wb3