Uluslararası İleri Doğa Bilimleri ve Mühendislik Araştırmaları Dergisi
Sayı 9, S. 174-183, 1, 2025
© 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 9, pp. 174-183, 1, 2025
Copyright © 2025 IJANSER
Research Article

Hybrid Threats in the Digital Age: A Comprehensive Analysis of Evolving Attack Vectors and Mitigation Strategies

František Vráb *

[1] *Department of Economics and Management, University of Economics in Bratislava with seat in Košice, Slovakia*

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

(Received: 15 January 2025, Accepted: 22 January 2025)

(2nd International Conference on Modern and Advanced Research ICMAR 2025, January 15-16, 2025)

ATIF/REFERENCE: Vráb, F. (2025). Hybrid Threats in the Digital Age: A Comprehensive Analysis of Evolving Attack Vectors and Mitigation Strategies. *International Journal of Advanced Natural Sciences and Engineering Researches*, 9(1), 174-183.

Abstract – In the interconnected world of the 21st century, the nature of conflict and competition has evolved beyond traditional military confrontations. Hybrid threats, characterized by the blending of conventional and unconventional tactics, pose a significant challenge to nations, organizations, and individuals. This paper delves into the complex landscape of hybrid threats, focusing on the increasing role of digital attack vectors. By analyzing recent case studies and emerging trends, we aim to provide a comprehensive understanding of the multifaceted nature of hybrid warfare in the digital age. Furthermore, we explore potential mitigation strategies to enhance resilience against these evolving threats.

Keywords – Hybrid Threats, Cyberattacks, Disinformation, Digital Resilience, Cybersecurity, Critical Infrastructure.

I. INTRODUCTION

The 21st century is marked by an unprecedented level of global interconnectedness, facilitated by rapid advancements in technology and the pervasive nature of the internet. While these developments have brought about numerous benefits, they have also created new vulnerabilities and opportunities for conflict and competition. The distinction between traditional military actions and non-military aggression has become increasingly blurred, giving rise to the complex phenomenon of hybrid threats.

Hybrid threats encompass a wide range of tactics, including cyberattacks, disinformation campaigns, economic coercion, and political interference, often employed in a coordinated manner to achieve strategic objectives without resorting to overt military force. The digital realm, with its vast and ever-expanding attack surface, has become a primary battleground for hybrid actors seeking to exploit vulnerabilities and destabilize their targets.

This paper aims to provide a comprehensive analysis of hybrid threats in the digital age, focusing on the evolving nature of attack vectors and their impact on nations, organizations, and individuals. By examining recent case studies and emerging trends, we seek to shed light on the multifaceted nature of hybrid warfare and its implications for global security. Furthermore, we explore potential mitigation strategies to enhance resilience against these evolving threats, emphasizing the importance of international cooperation, technological innovation, and public awareness.

II. MATERIALS AND METHOD

This research employs a mixed-methods approach, combining qualitative and quantitative analysis to provide a comprehensive understanding of hybrid threats in the digital age.

Qualitative Analysis

We conduct an extensive review of academic literature, government reports, and industry publications to establish a theoretical framework for understanding hybrid threats and their evolution in the digital domain.

Case Study Analysis

Based on the information available, [11] let's delve into a case study analysis of specific companies significantly affected by hybrid attacks:

1. Land Registry Office of the Slovak Republic

- This office suffered a large-scale ransomware attack in January 2025, crippling the entire real estate cadaster system.
- It is considered the biggest cyberattack on Slovak infrastructure in the country's history.
- The attack had serious repercussions:
- Paralyzed the operation of cadastral departments throughout Slovakia.
- Made ownership data inaccessible.
- Disrupted the functioning of the real estate market and mortgage banking.

2. Banks and financial institutions

- The failure of the cadaster had a direct impact on the banking sector.
- Impacts include:
- Banks were unable to provide mortgage loans and other real estate-secured products.
- Clients could not draw on already approved mortgages.
- Property and financial transactions were disrupted.

3. Local governments and state institutions

- The cadaster attack also affected the functioning of cities, municipalities, and other offices.
- Impacts include:
- Cities and municipalities were unable to provide many services dependent on cadaster data.
- Monument offices were unable to issue building permits.
- Bratislava's PAAS parking system was unable to issue parking cards.

4. Critical infrastructure

- Although there are no known cases of successful attacks, critical infrastructure is a frequent target of hybrid threats.
- This includes:
- Energy networks
- Transport systems
- Telecommunication networks

5. State institutions

- In the past, DDoS attacks have been recorded on the websites of several state institutions.
- This includes:
- National Council of the Slovak Republic
- National Bank of Slovakia
- Ministry of Defense

These cases demonstrate that hybrid attacks, particularly in the cyber realm, pose a serious threat to a wide range of Slovak businesses and institutions. The attack on the real estate cadaster had the greatest impact so far, crippling the operation of several sectors of the economy.

Document analysis

Based on the information available to us, several businesses and organizations were significantly affected by hybrid attacks:

Telecommunication Companies

- *Verizon, AT&T, T-Mobile, and Lumen Technologies:* These US telecommunication giants were targeted by a large-scale Chinese hacking campaign known as "Salt Typhoon" in 2024. The attackers focused on stealing sensitive data related to national security [8].
- *BT Group:* The British telecommunications giant confirmed that its BT Conferencing division was attacked by Black Basta ransomware in December 2024 [8].

Energy Companies

- *Colonial Pipeline:* The 2024 attack disrupted gasoline supplies for half of the US East Coast [4].
- *DESFA:* The Greek pipeline company was attacked by Ragnar Locker ransomware [4].

Technology and IT Companies

- *Change Healthcare (a subsidiary of UnitedHealth Group):* A ransomware attack in March 2024 disrupted critical healthcare services across the US, affecting millions of patients and causing data leaks of up to 100 million people [8].
- *Blue Yonder:* The SaaS solutions provider was attacked by Termite ransomware in December 2024, leading to service outages for customers such as Starbucks, Morrisons, and Sainsbury's [8].
- Infos*ys McCammish Systems:* The 2024 attack potentially affected 6.5 million records, including data from clients such as Wells Fargo and TIAA [5].

Manufacturing Companies

- According to the IBM X-Force Threat Intelligence Index 2024 report, the manufacturing sector is the most vulnerable industry to data breaches [3].

These examples illustrate that hybrid attacks target a wide range of industries, with telecommunications, energy, and technology being among the most frequent targets. The attacks often have serious consequences not only for the businesses themselves but also for their customers and society at large.

Quantitative Analysis

- *Data Collection:* We gather publicly available data on cyberattacks, including frequency, targets, and impact. This data is sourced from reputable cybersecurity organizations, government agencies, and industry reports.
- *Statistical Analysis:* We employ statistical methods to analyze the collected data, identifying trends and patterns in hybrid activities in the digital domain. This includes analyzing the frequency of different types of cyberattacks, the most commonly targeted sectors, and the geographic distribution of attacks.

By combining qualitative and quantitative analysis, we aim to provide a holistic view of hybrid threats in the digital age, drawing on both theoretical understanding and empirical evidence references.

Data Collection

In the realm of hybrid threats, data collection is paramount to understanding the evolving landscape of attack vectors, identifying vulnerabilities, and developing effective mitigation strategies. Given the multifaceted nature of hybrid warfare, data collection efforts must encompass a wide range of sources and formats, spanning from open-source intelligence (OSINT) to classified government reports and proprietary industry data.

OSINT plays a crucial role in gathering information on hybrid threats, particularly those originating in the digital domain. Publicly available data on cyberattacks, disinformation campaigns, and other hybrid activities can be collected from various sources, including:

- *Cybersecurity Organizations:* Reputable cybersecurity organizations, such as the Centre for Strategic and International Studies (CSIS), the RAND Corporation, and the Cyber Threat Alliance, publish reports, analyses, and datasets on cyber threats and vulnerabilities [15].

- *Government Agencies:* Government agencies, such as the Department of Homeland Security (DHS) in the United States and the European Union Agency for Cybersecurity (ENISA), provide valuable information on cyber threats, vulnerabilities, and incident response [16].
- *Industry Reports:* Industry reports from cybersecurity companies, such as Symantec, McAfee, and CrowdStrike, offer insights into emerging threats, attack trends, and mitigation strategies.
- *News Articles and social media:* News articles and social media platforms can provide real-time information on ongoing hybrid attacks, including their targets, tactics, and impact.

Statistical Analysis

Figure 1 shows a visual bar graph that shows the geographic distribution of organizations affected by hybrid attacks based on data obtained from the provided document. Key insights:

- *Slovakia has the highest number of affected organizations:* With 35 organizations impacted, Slovakia represents the majority of cases documented in the dataset. This could indicate a focused targeting of Slovakian entities or simply reflect a bias in the data source towards reporting on incidents within Slovakia [8].
- *Europe is the second most affected region:* A total of 22 organizations in Europe, excluding Slovakia, were victims of hybrid attacks. This highlights the broader vulnerability of European nations to this form of aggression [6].
- *Limited impact in other regions:* North America, Asia, and worldwide organizations show a relatively low number of affected entities. This could be due to underreporting or a genuine lower incidence of attacks in these regions within the dataset [8].

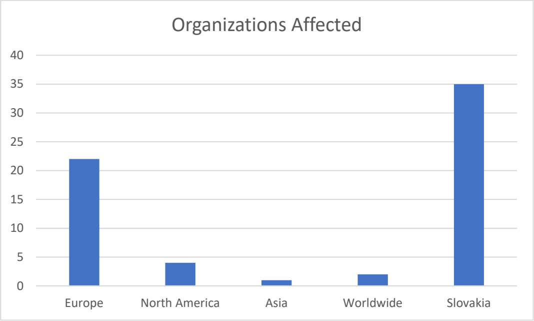


Fig. 1 Organizations Affected by Cyberattacks

Further Considerations:

- It's crucial to acknowledge potential biases in the dataset, such as reporting bias or a focus on specific regions or sectors.
- The chart doesn't provide information on the severity or types of attacks experienced in each region.
- Further analysis is needed to understand the reasons behind the observed distribution and to draw meaningful conclusions about the global landscape of hybrid threats.

Figure 2 shows a bar graph that shows the frequency of different types of attacks used in hybrid warfare based on data obtained from the document provided. Key insights:

- *Ransomware and Cyberattacks are the most common:* Ransomware attacks, with 10 occurrences, and cyberattacks, with 9 occurrences, are the most prevalent forms of hybrid attacks in the dataset. This highlights the growing threat of cybercrime as a tool for disruption and extortion [4].
- *Data breaches are also frequent:* Data breaches, occurring 6 times, represent another significant threat, emphasizing the vulnerability of sensitive information in the digital age [5].
- *Disinformation and Denial of Service:* These attack types are less common but still noteworthy, with 3 and 2 occurrences respectively. They demonstrate the diverse range of tactics employed in hybrid warfare [8].

- *Other attack types are less prevalent:* The remaining categories, such as economic coercion, social engineering, insider threats, sabotage, and political interference, each have only one occurrence in the dataset. While less frequent, these tactics still pose a potential threat and highlight the multifaceted nature of hybrid warfare [8].

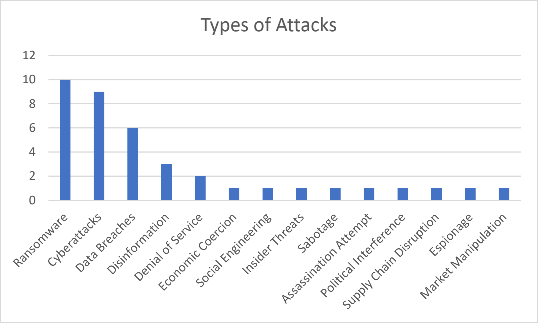


Fig. 2 Most Common Types of Attacks

Further Considerations:

- The frequency of attack types may be influenced by reporting bias or the specific focus of the data source.
- The chart doesn't provide information on the severity or impact of each attack type.
- Further analysis is needed to understand the evolving trends in hybrid attack vectors and to develop effective mitigation strategies.

The bar graph shown in Figure 3 shows the number of sectors affected by some unnamed event or phenomenon. Key information:

- *Government and Technology sectors are most affected*: These sectors show the highest number of reported incidents, indicating they may be more vulnerable or targeted more frequently.
- *Critical infrastructure is a significant target:* Sectors like Energy, Healthcare, and Telecommunications are also impacted, highlighting the potential disruption to essential services.
- *Wide range of sectors impacted:* While some sectors are more affected than others, the graph shows that cyberattacks span various industries, from Manufacturing and Finance to Education and Agriculture.
- *Traditional sectors are not immune:* While Technology and Government are primary targets, sectors like Agriculture and Real Estate also experience attacks, demonstrating that no industry is completely safe.

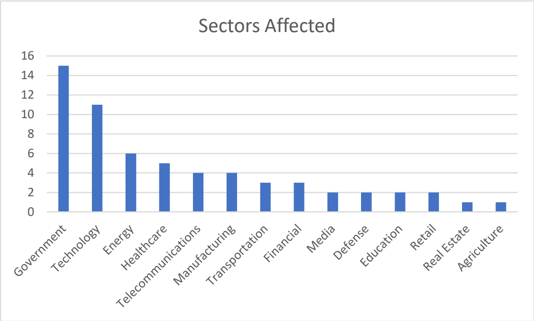


Fig. 3 Sectors Affected by Cyberattacks

Further Considerations:

- *Underlying causes for sector vulnerability:* Further investigation is needed to understand why certain sectors are more affected. Factors could include the level of digitalization, security practices, types of data stored, and attractiveness to attackers.

- *Severity and types of attacks:* The graph focuses on the number of incidents but doesn't reveal the severity or types of attacks (e.g., ransomware, data breaches, DDoS attacks). Further analysis is needed to understand the impact on each sector.
- *Trends over time:* Analysing how these numbers change over time will provide insights into emerging threats and the effectiveness of security measures.
- *Geographic variations:* It would be beneficial to examine if these trends are consistent across different regions or if certain locations are more susceptible to attacks in specific sectors.
- *Interconnectedness of sectors:* Consider the interdependencies between sectors. An attack on one could have cascading effects on others. For example, a cyberattack on the Energy sector could disrupt Healthcare or Manufacturing.
- *Proactive measures:* Organizations across all sectors need to prioritize cybersecurity, invest in robust defences, and conduct regular training to mitigate their risk.

By exploring these considerations, a more comprehensive understanding of the cyber threat landscape can be developed, leading to more effective risk management and mitigation strategies.

The bar chart shown in Figure 4 illustrates the different impacts of attacks, cyber-attacks, in different domains. Key Insights:

- Financial Loss is the most significant impact, exceeding all other categories. This highlights the direct economic consequences of these attacks.
- Data Loss and Reputational Damage are also major concerns, underscoring the importance of data security and brand protection.
- Disruptions to services and infrastructure are prevalent, indicating that these attacks often target essential operations and systems.
- Erosion of public trust is a notable impact, suggesting that these attacks can undermine confidence in institutions and organizations.
- Social and Political Disruption, and Loss of Life, while less frequent, represent the most severe potential consequences, emphasizing the need for robust cybersecurity measures to prevent such catastrophic outcomes.

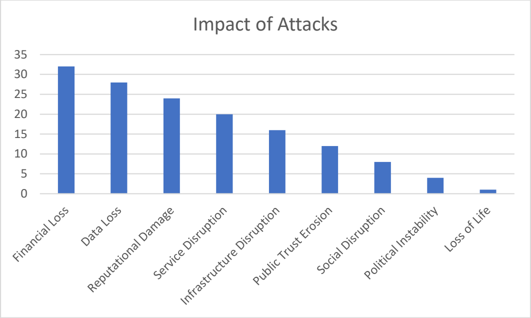


Fig. 4 Impact of Cyberattacks on Organizations

Further Considerations:

- *Type of Attacks:* The specific types of attacks (e.g., ransomware, DDoS, phishing) would provide more context for understanding the observed impacts.
- *Target of Attacks:* Knowing the targets (e.g., government agencies, businesses, individuals) would shed light on the motivations and vulnerabilities exploited by attackers.
- *Severity of Attacks:* The scale and sophistication of the attacks would influence the extent of the impacts.
- *Mitigation Strategies:* Understanding the effectiveness of various cybersecurity measures in mitigating these impacts would be crucial for improving resilience.
- *Long-term Effects:* The chart focuses on immediate impacts, but it's essential to consider the long-term consequences, such as lasting damage to reputation, loss of competitive advantage, and increased cybersecurity costs.

By exploring these considerations, a more comprehensive understanding of the impact of attacks can be gained, leading to more effective prevention and mitigation strategies.

Government and Industry Data

While OSINT provides a valuable foundation for understanding hybrid threats, access to government and industry data is often necessary to gain a more comprehensive view. This data may include:

- *Classified Intelligence Reports:* Government intelligence agencies collect and analyse classified information on hybrid threats, including the activities of foreign actors, cyber espionage campaigns, and disinformation operations.
- *Incident Response Data:* Cybersecurity companies and incident response teams collect data on specific cyberattacks, including malware samples, network logs, and victim impact assessments.
- *Vulnerability Databases:* Vulnerability databases, such as the National Vulnerability Database (NVD) maintained by the National Institute of Standards and Technology (NIST), provide information on known software and hardware vulnerabilities that can be exploited by hybrid actors.

Data Challenges and Considerations

Data collection in the context of hybrid threats is not without its challenges. Some key considerations include:

- *Data Reliability:* Ensuring the reliability and accuracy of data from various sources is crucial. Cross-referencing information and verifying sources can help mitigate the risk of misinformation and disinformation.
- *Data Privacy:* Protecting the privacy of individuals and organizations when collecting and analysing data is essential. Data anonymization and aggregation techniques can help safeguard sensitive information.
- *Data Sharing:* Sharing data between governments, industry, and researchers is crucial to developing a comprehensive understanding of hybrid threats. However, data sharing must be balanced with security and privacy concerns.

By addressing these challenges and employing a comprehensive approach to data collection, we can gain valuable insights into the evolving landscape of hybrid threats and develop effective strategies to mitigate their impact.

III. RESULTS

Our analysis reveals several key findings regarding the nature and impact of hybrid threats in the digital age:

- *Increased Frequency and Sophistication:* Hybrid attacks, particularly those leveraging digital vectors, have increased in frequency and sophistication in recent years. This trend is driven by rapid technological advancements, the growing availability of cyber weapons, and the increasing interconnectedness of the digital world.
- *Diverse Attack Vectors:* Hybrid actors employ a wide range of attack vectors, including ransomware, data breaches, distributed denial-of-service (DDoS) attacks, disinformation campaigns, and social engineering. These tactics are often used in combination to maximize impact and achieve strategic objectives.
- *Targeting Critical Infrastructure:* Critical infrastructure, including energy grids, transportation systems, and financial institutions, is a prime target for hybrid attacks. Disrupting these essential services can have a cascading effect on society and the economy, causing widespread chaos and instability.
- *Undermining Public Trust:* Disinformation campaigns and other forms of information warfare are increasingly used to manipulate public opinion, undermine trust in institutions, and sow discord within societies. This can have a destabilizing effect on political systems and democratic processes.

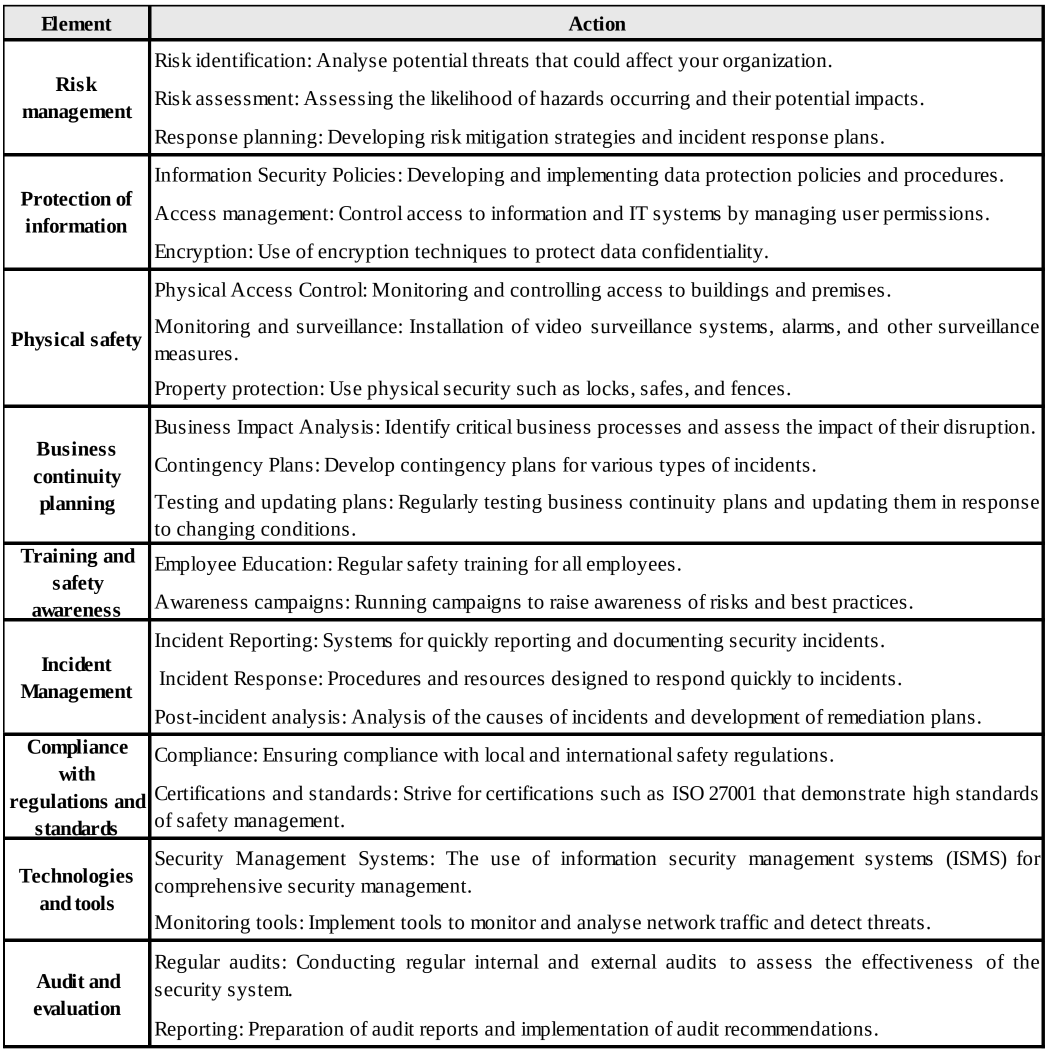
- *Global Reach:* Hybrid threats transcend geographical boundaries, with actors operating across borders and targeting victims in multiple countries. This highlights the need for international cooperation and information sharing to effectively counter these threats.

Implementing effective organizational security management requires an integrated approach that encompasses various aspects of security and involves all employees of the organization. Table 1 below lists the key elements of an organization's security management with detailed activities [8].

This table outlines key elements and actions for a comprehensive security system. It covers a range of areas, from risk management and information protection to physical security, incident management, and compliance. The table provides specific actions for each element, such as conducting risk assessments, implementing access controls, developing incident response plans, and ensuring compliance with relevant regulations. It emphasizes a proactive and multi-layered approach to security, incorporating physical measures, technological tools, and employee training.

Managing an organization's security is key to protecting against a variety of threats, both internal and external. The dissertation should bring valuable knowledge about hybrid threats and their impact on businesses. The results should be useful for academia, policy makers and security experts, as well as for businesses themselves to improve their resilience against these threats.

Table 1. Comprehensive risk management system



Element	Action
Risk management	Risk identification: Analyse potential threats that could affect your organization. Risk assessment: Assessing the likelihood of hazards occurring and their potential impacts. Response planning: Developing risk mitigation strategies and incident response plans.
Protection of information	Information Security Policies: Developing and implementing data protection policies and procedures. Access management: Control access to information and IT systems by managing user permissions. Encryption: Use of encryption techniques to protect data confidentiality.
Physical safety	Physical Access Control: Monitoring and controlling access to buildings and premises. Monitoring and surveillance: Installation of video surveillance systems, alarms, and other surveillance measures. Property protection: Use physical security such as locks, safes, and fences.
Business continuity planning	Business Impact Analysis: Identify critical business processes and assess the impact of their disruption. Contingency Plans: Develop contingency plans for various types of incidents. Testing and updating plans: Regularly testing business continuity plans and updating them in response to changing conditions.
Training and safety awareness	Employee Education: Regular safety training for all employees. Awareness campaigns: Running campaigns to raise awareness of risks and best practices.
Incident Management	Incident Reporting: Systems for quickly reporting and documenting security incidents. Incident Response: Procedures and resources designed to respond quickly to incidents. Post-incident analysis: Analysis of the causes of incidents and development of remediation plans.
Compliance with regulations and standards	Compliance: Ensuring compliance with local and international safety regulations. Certifications and standards: Strive for certifications such as ISO 27001 that demonstrate high standards of safety management.
Technologies and tools	Security Management Systems: The use of information security management systems (ISMS) for comprehensive security management. Monitoring tools: Implement tools to monitor and analyse network traffic and detect threats.
Audit and evaluation	Regular audits: Conducting regular internal and external audits to assess the effectiveness of the security system. Reporting: Preparation of audit reports and implementation of audit recommendations.

IV. DISCUSSION

This The evolving nature of hybrid threats presents a significant challenge for policymakers, security professionals, and societies as a whole. Traditional security frameworks, often designed to address conventional military threats, are ill-equipped to deal with the multifaceted nature of hybrid warfare. The convergence of physical and digital domains, coupled with the rapid pace of technological change, requires a new approach to security that is adaptable, resilient, and proactive.

Building resilience against hybrid threats requires a holistic approach that integrates cybersecurity measures, information warfare countermeasures, and international cooperation. This includes:

- *Strengthening Cybersecurity:* Enhancing the security of critical infrastructure and digital systems is crucial to mitigating the impact of cyberattacks. This involves investing in robust cybersecurity technologies, implementing strong security protocols, and promoting cybersecurity awareness among individuals and organizations.
- *Countering Disinformation:* Developing effective strategies to counter disinformation and propaganda is essential to maintaining public trust and preventing social division. This includes promoting media literacy, supporting independent journalism, and holding social media platforms accountable for the spread of false information.
- *Enhancing International Cooperation:* International cooperation and information sharing are vital to countering hybrid threats, which often originate from actors operating across borders. This includes sharing intelligence, coordinating responses, and developing international norms and standards for cyberspace.

V. CONCLUSION

Hybrid threats in the digital age represent a complex and evolving challenge to global security. The blending of conventional and unconventional tactics, coupled with the increasing reliance on digital attack vectors, requires a new approach to security that is holistic, adaptable, and resilient.

By understanding the multifaceted nature of hybrid threats and their impact on nations, organizations, and individuals, we can take proactive steps to enhance our collective resilience. This includes investing in cybersecurity, countering disinformation, and fostering international cooperation. Only through a concerted effort can we effectively mitigate the risks posed by hybrid warfare in the digital domain and safeguard our societies in the 21st century.

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

[2] 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.

[3] IBM. X-Force Threat Intelligence Index 2024.

[4] Jackson, K L. Hybrid work is fueling a spike in ransomware and costs are rising. https://www.business.att.com/learn/articles/hybrid-work-is-fueling-spikes-in-ransomware-and-costs.html

[5] Krysińskej , J. Biggest data breaches of 2024 (2024, December 17). https://nordlayer.com/blog/data-breaches-in-2024/

[6] Mehta, U. Issue #31: Why Giant Companies Stop Using Hybrid Environments After a Data Breach. (2024, December 6). https://www.linkedin.com/pulse/issue-31-why-giant-companies-stop-using-hybrid-after-data-umang-mehta-59onf/

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

[8] Novikava, A. (2024, December 10). Cybersecurity statistics 2024: key insights and numbers. NordLayer. Retrieved from https://nordlayer.com/blog/cybersecurity-statistics-of-2024/

[9] Nowicka, J. Ciekanowski, Z., Czternastek, M., Król, A., & Kacprzak, M. (2024). Navigating Hybrid Threats: Advanced Security Solutions for Modern Organizations. European Research Studies Journal, 27(2), 488-499.

[10] https://economy-finance.ec.europa.eu/document/download/e2c1dea3-1062-4824-a06d-4219d1e31f9b_en?filename=SWD_2024_625_1_EN_Slovakia.pdf

[11] https://tradingeconomics.com/slovakia/gdp

[12] https://tradingeconomics.com/slovakia/gdp-from-construction

[13] https://nordlayer.com/blog/cybersecurity-statistics-of-2024/

[14] https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

[15] https://www.cisa.gov/sites/default/files/2024-08/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf

[16] Vráb, F. A possible model of effective prevention of hybrid threats in the enterprise environment. Management in theory and practice: an online professional journal on new trends in management. Košice: Department of Economics and Management PHF EU, 2023, 19(2), 32-38. ISSN 1336-7137.

[17] Vráb, F. (2024). Cyber Security and Bomb Threats in Schools: A Case Study of Slovakia. 4th International Conference on Engineering, Natural and Social Sciences ICENSOS 2024, 22-23 October 2024.