American Journal of Research, Education and Development

RED

ISSN 2471-9986

American Journal of Research, Education and Development

IMPRESSUM

American Journal of Research, Education and Development
ISSN: 2471-9986

Publisher: DEVLART LLC
250 Camelback Ridge Ave. Henderson, NV 89012
red@devlart.hu

Editor in Chief:
dr. habil Gyula KÓRÓDI MD. PhD

Managing Editor:
Dr. János RIKK

Editorial Secretary:
Géza HORVÁTH

Table of Content

Enhancing Military Cyber Defense: The Role of Threat Intelligence in Military Security Operations Centers

Timea Pahi (ORCID: 0000-0001-7346-3450)

Ludovika University of Public Service

Andras Toth (ORCID: 0000-0001-6098-3262)

Ludovika University of Public Service

The potential of cybersecurity exercises in critical infrastructures

Timea Pahi (ORCID: 0000-0001-7346-3450)

Ludovika University of Public Service

Andras Toth (ORCID: 0000-0001-6098-3262)

Ludovika University of Public Service

Habits that can be acquired during the training and their effects in disaster protection

MUHORAY, Róbert András, Doctoral School of Military Sciencies, PhD student. ORCID: 0000-0002-8440-6133

Assessment of Public Security Planning Regulations and Guidlines related to Dangerous Goods Transportation Facilities

Zoltán Cséplő PhD, chief inspector, Capital Disaster Management Directorate, Budapest, Hungary, zoltan.cseplo@katved.gov.hu *ORCID: 0000-0002-8920-3095*

American Journal of Research, Education and Development
ISSN 2471-9986
2024/3

Enhancing Military Cyber Defense: The Role of Threat Intelligence in Military Security Operations Centers

Timea Pahi (ORCID: 0000-0001-7346-3450)
Ludovika University of Public Service

Andras Toth (ORCID: 0000-0001-6098-3262)
Ludovika University of Public Service

Abstract

As cyber threats evolve, the need for robust cybersecurity frameworks in military operations has become increasingly imperative. Threat Intelligence (TI) plays a crucial role in fortifying military Security Operations Centers (SOCs) by providing actionable insights into adversarial tactics, techniques, and procedures (TTPs). This paper extends previous research on TI metrics by incorporating a military perspective, emphasizing the application of cyber threat intelligence in military SOCs, its integration with existing defense infrastructure, and its role in enhancing operational readiness. The methodology for selecting threat intelligence metrics is adapted to military environments, highlighting the strategic, tactical, and operational significance of TI in modern warfare. The key finding of this paper was that TI metrics need to be changed to work in military settings. It's time for a new way to measure and evaluate cybersecurity because the old ways don't work well with the operational realities of military cyber defense. This paper introduced five SOC metrics that are specific to the military and are meant to deal with these specific problems.

1. Introduction

Cyber warfare has become a critical component of modern military strategy, with nation-states and non-state actors leveraging sophisticated cyber techniques to disrupt defense systems. The term cybersecurity has nearly become synonymous with safety for industries, nation-states, and individuals alike. Cyber threats are rapidly evolving and becoming increasingly sophisticated, creating chokepoints for many industries undergoing digitalization. In this dynamic environment, it is essential to implement innovative strategies to effectively reduce cyber risks. The tactics utilized by cybercriminals have evolved beyond traditional cybercrimes, encompassing supply chain attacks and insider threats, thereby necessitating a comprehensive approach to organizational security.

Military organizations require advanced threat intelligence capabilities to detect, analyze, and mitigate cyber threats in real time. Unlike commercial enterprises, military SOCs must address unique challenges such as classified data protection, coordination with intelligence agencies, and the integration of cyber defense within broader military operations. Recognizing the growing significance of cyber threats, NATO has established a comprehensive cyber defense policy to enhance collective resilience and operational readiness. The policy emphasizes a proactive approach, integrating cyber defense measures into overall military strategies to ensure the protection of critical infrastructure and

strategic assets[1]. Organizations have attempted to counter cyber threats by either maintaining in-house Security Operations Centers (SOCs) or outsourcing cybersecurity services to enhance their defense capabilities. SOCs play a central role in maintaining an organization's security posture by detecting security incidents and responding to them effectively. However, designing an optimal SOC architecture that aligns with organizational needs and budget constraints remains a significant challenge[2]. Different architectures offer various advantages, but their effectiveness depends on multiple factors, as highlighted by Vielberth et al[3].

To bring a certain degree of uniformity to SOC operations, reliable threat intelligence data is necessary. Cyber Threat Intelligence (CTI) is a multidimensional resource that aids in identifying threat actors, their motives, preferred targets, and attack history. Despite its evident advantages, CTI adoption remains relatively low, even in sectors that would benefit the most[4]. Its implementation is often driven by IT operations staff rather than higher-level decision-makers[5]. Additionally, sharing TI among peers enhances situational awareness and strengthens the overall security posture of organizations[6].

To achieve a robust TI infrastructure, the integration of appropriate metrics is crucial. Unfortunately, there is a significant lack of standardized metrics that can be applied across domains, as well as limited methodologies for evaluating existing metrics. The research presented in this paper builds upon existing methodologies for TI metric selection and adapts them for military applications, ensuring that the intelligence gathered is both reliable and actionable[7]. We explore a framework built upon established principles used to measure different types of metrics and select the most relevant ones based on their applicability in military environments[8]. Furthermore, we address ambiguities in metric selection, such as the interpretation of 'mean time to detect,' which may vary depending on its context within a SOC environment.

2. The Role of Threat Intelligence in Military Operations

[1] Bányász, P., Krasznay, C., & Tóth, A. (2021). A NATO kibervédelmi szakpolitikája. (in Hungarian) in A mai NATO, 130-149.

[2] Cyber Strategy Institute. (2025, January 9). Gartner Analysis of Security Operations Centers (SOCs) in 2024 - Understanding the Hype CycleTM for Security. https://cyberstrategyinstitute.com/gartner-analysis-of-securityoperations-centers-socs-in-2024-understanding-the-hypecycle-for-security-operations/

[3] Vielberth, M., Bohm, F., Fichtinger, I., Pernul, G. (2020). Security Operations Center: A systematic study and open challenges. IEEE Access, 8, 227756–227779. https://doi.org/10.1109/access.2020.3045514

[4] Kotsias, J., Ahmad, A., & Scheepers, R. (2023). Adopting and integrating cyber-threat intelligence in a commercial organisation. European Journal of Information Systems, 32(1), 35-51.

[5] Ainslie, S., Thompson, D., Maynard, S., Ahmad, A.(2023). Cyber-threat intelligence for security decision-making: A review and research agenda for practice. Computers Security, 132, 103352. https://doi.org/10.1016/j.cose.2023.103352

[6] Alaeifar, P., Pal, S., Jadidi, Z., Hussain, M., Foo, E. (2024). Current approaches and future directions for Cyber Threat Intelligence sharing: A survey. Journal of Information Security and Applications, 83, 103786. https://doi.org/10.1016/j.jisa.2024.103786

[7] E. Agyepong, Y. Cherdantseva, P. Reinecke and P. Burnap, "Towards a Framework for Measuring the Performance of a Security Operations Center Analyst," 2020 International Conference on Cyber Security and Protection of Digital Services (Cyber Security), Dublin, Ireland, 2020, pp. 1-8, doi:10.1109/CyberSecurity49315.2020.9138872.

[8] Ahlm, Eric. "How to build and operate a modern security operations center." Gartner Inc (2021).

Threat intelligence in military environments goes beyond conventional cybersecurity practices by incorporating strategic foresight into national defense planning. The military employs TI at three levels:

- **Strategic Intelligence:** Informs high-level decision-making by providing insights into cyber threats posed by nation-state actors, geopolitical trends, and emerging vulnerabilities in defense infrastructure.
- **Tactical Intelligence:** Supports military SOCs by analyzing threat actor behavior, malware signatures, and vulnerabilities that could be exploited in cyber warfare.
- **Operational Intelligence:** Enables real-time monitoring and response to cyber incidents, ensuring mission continuity and system integrity during active operations.

Military SOCs utilize TI to proactively defend against cyber adversaries by leveraging cyber threat frameworks such as MITRE ATT&CK and structured analytic techniques. This approach enhances situational awareness and ensures that military units can preemptively counteract cyber threats before they escalate.

2.1 Selecting a metric for SOC

As defined by Herrmann in the context of security metrics[9]: 'Metric: a proposed measure or unit of measure that is designed to facilitate decision making and improve performance and accountability through collection, analysis, and reporting of relevant data.' Generally, it is the measurement of values in discreet point in time. we start by gathering metrics pertaining to particular entities' properties. An entity is an events or an object in real world. An entity's characteristic or property is called an attribute.

A metric must validate these requirements: 1. The goal for selecting the metric should be well defined. 2. The metric should have one or more distinct functions. 3. The metric should not depend on a specific technology or source. 4. The metric should not be sourced by illegal sources and or for result in legal infringements. 5. The metric should conform to the mentioned characteristics. Since there is a lack of standardized set of requirements, we have sourced the essential conditions that need to be met, from PRAGMATIC framework[10] and Foosberg et. al[11].

As discussed before a metric should be able to define an entity as precisely as possible. The characteristic must showcase the behavioral attributes of a said entity. The following characteristics would help provide a better understanding of a given entity we wish to evaluate to check its own validity.

We have skimmed through the characteristics provided by Herrmann[8] to suit the needs for TI and they are as follows:

---

[9] Herrmann, D. S. (2007). Complete guide to security and privacy metrics. In Auerbach Publications eBooks.https://doi.org/10.1201/9781420013283

[10] Brotby, W. Krag, and Gary Hinson. Pragmatic security metrics: applying metametrics to information security. CRC Press, 2016.

[11] Forsberg, J., Frantti, T. (2023). Technical performance metrics of a security operations center. Computers Security, 135, 103529. https://doi.org/10.1016/j.cose.2023.103529

1. Accuracy: According to the standard unit of measurement established by the measurement procedure, accuracy denotes that the measurement of a characteristic was true or exact.

2.Validity: The question of whether a metric actually measures what it was designed to measure is another facet of validity.

3.Correctness: It implies that the data was gathered in compliance with the precise guidelines specified in the metric. The level of formality that was followed during the measurement process is reflected in correctness.

2.2 Adapting TI Metrics for Military Use

Adapting TI metrics for military environments necessitates a tailored approach that is consistent with mission-critical objectives and operational needs. Traditional cybersecurity metrics must be reconsidered to ensure that they account for the unique nature of military cyber operations. The main components of military-specific TI metrics are:

Mission Impact Analysis: Military SOCs must evaluate the operational consequences of cyber threats, with a focus on intelligence that directly affects mission readiness, command structures, and battlefield decision-making. Metrics should assess the speed, accuracy, and reliability of threat detection and mitigation.

Adversarial Attribution: Military decision-making relies heavily on the ability to confidently identify threat actors. Attribution metrics must assess the efficacy of forensic techniques, threat profiling accuracy, and the success rate in distinguishing between state-sponsored actors, terrorist groups, and independent cybercriminals.

Operational Resilience Metrics: Unlike commercial environments, military SOCs must maintain operational continuity in the face of sustained cyberattacks. Metrics should be used to assess downtime, the efficacy of redundant systems, and the effectiveness of incident response procedures in ensuring critical communications and infrastructure.

Threat prediction and intelligence sharing: Proactive defense is critical in military operations. Metrics should evaluate predictive analytics' accuracy in forecasting attack vectors, as well as the effectiveness of intelligence-sharing mechanisms between allied forces and defense agencies.

By developing and refining these metrics, military SOCs can improve their ability to detect, analyze, and respond to threats while remaining consistent with overall national security strategies.

2.4 Five Military-Specific Metrics for Security Operations Centers (SOCs)

Unlike civilian cybersecurity environments, military SOCs operate under unique conditions that require specialized threat intelligence metrics. These metrics must align with national security

objectives, ensure operational resilience, and support mission-critical decision-making[12]. A cyber incident that disrupts the communication systems essential for command and control would be assigned a significantly high severity score, as it directly affects the successful execution of military operations. In contrast, a less critical threat, such as an attack on weather forecasting sensors, would receive a lower score, indicating that it does not pose a mission-critical risk and primarily impacts a subordinate system. This scoring framework enables military leaders and decision-makers to identify the most significant risks to operational success promptly. Consequently, it enhances their capacity to allocate resources efficiently and respond appropriately to mitigate threats, thereby ensuring the integrity of operations.

Below are five key military-specific metrics that enhance the effectiveness of military SOCs:

1. Mission Impact Score (MIS)

Definition: Measures the direct impact of a cyber threat on military operations and mission readiness.

Explanation: Unlike traditional risk assessments that focus on financial or reputational loss, military SOCs must evaluate cyber threats based on their potential to disrupt critical missions. The MIS assigns a score to cyber incidents based on factors such as system criticality, operational dependencies, and time-sensitive objectives. A higher score indicates a greater risk to mission success, allowing decision-makers to prioritize responses accordingly.

2. Adversarial Attribution Confidence Index (AACI)

Definition: Quantifies the accuracy and reliability of identifying the threat actor behind a cyber attack.

Explanation: Military cybersecurity operations require precise attribution of adversaries, whether nation-state actors, cybercriminals, or insurgent groups. The AACI measures the effectiveness of forensic analysis, threat intelligence correlation, and pattern recognition in identifying attackers. A high confidence score improves response strategies, enabling military decision-makers to deploy appropriate countermeasures or escalate to diplomatic or kinetic actions. Forensic analysis involves systematically examining and evaluating digital evidence obtained from various cyber incidents to identify and trace the origins and methodologies employed by attackers. Identifying malicious actors and their tactics, techniques, and procedures (TTP) can be accomplished through the correlation of threat intelligence. This process encompasses the collection and analysis of data from a diverse range of sources. Experts apply algorithms and machine learning techniques for pattern recognition, which aids in the detection of recurring behaviors and anomalies that may assist in determining the identities of attackers. By utilizing the AACI, professionals can implement appropriate countermeasures with heightened effectiveness. These countermeasures may include fortifying cyber defenses, conducting offensive cyber operations, or, if warranted, initiating

[12] Smeets, M. (2022). No shortcuts: Why states struggle to develop a military cyber-force. Oxford University Press.

diplomatic or kinetic responses. Accurate attribution is essential for enhancing cybersecurity measures and significantly contributes to achieving broader national security objectives.

3. Cyber-Kinetic Convergence Index (CKCI)

Definition: Assesses the likelihood and severity of a cyber threat affecting physical military assets or operations.

Explanation: Military operations increasingly integrate cyber and kinetic warfare, where cyberattacks can disrupt radar systems, satellite communications, or weapons platforms. The CKCI evaluates threats based on their ability to cause tangible damage. Cyber attacks represent a significant threat to military equipment and systems, potentially resulting in considerable physical damage. For instance, an attack that disrupts communication or GPS signals for a military drone may lead to its crash. Furthermore, an attack on a weapon system could disable the platforms facilitating the firing mechanisms, thereby rendering the weapons inoperative. Additionally, targeting a combat vehicle by shutting down its engine or cooling systems may cause catastrophic failures, including the risk of explosion. This metric helps military SOCs determine which cyber threats require immediate mitigation to prevent cascading effects on battlefield operations.

4. Secure Information Exchange Effectiveness (SIEE)

Definition: Measures the efficiency and security of cyber threat intelligence sharing among military branches, allies, and intelligence agencies.

Explanation: Military SOCs rely on intelligence-sharing networks to enhance collective defense and ensure coordinated responses to cyber threats. The SIEE assesses the speed, accuracy, and security of TI dissemination, including compliance with protocols like Structured Threat Information eXpression (STIX) and Trusted Automated eXchange of Intelligence Information (TAXII). STIX is a standardized language that enables the interpretation of TI information across various systems. This uniformity allows different military systems and SOCs to effectively understand the information disseminated through alliance systems. In addition, TAXII is a transport protocol designed to facilitate the secure exchange of this information among disparate military networks. High effectiveness scores indicate a well-integrated intelligence-sharing ecosystem, reducing response time and improving collaborative cyber defense efforts.

5. Operational Resilience Index (ORI)

Definition: Evaluates the military SOC's ability to maintain functionality during sustained cyberattacks.

Explanation: Unlike commercial SOCs, military cybersecurity teams must continue operating even under persistent and coordinated cyberattacks. The ORI measures factors such as system redundancy, automated recovery processes, and the effectiveness of defensive cyber operations (DCO). The ORI serves to evaluate the capacity of the existing military systems to incorporate backup systems and components that ensure continued functionality in the event of primary system failures. This index elucidates the effectiveness of automated recovery processes in swiftly restoring systems

to operational status, thereby minimizing downtime and enabling rapid responses to incidents. Furthermore, the efficacy of DCO is assessed to determine whether the implemented measures and strategies are capable of detecting, preventing, and responding to cyber threats. Key components of this evaluation include the utilization of real-time threat intelligence, monitoring systems such as intrusion detection systems, and the establishment of rapid incident response teams. A higher ORI score indicates a stronger ability to withstand cyber disruptions and maintain command and control (C2) capabilities in contested environments.

With these five military-specific SOC metrics, you can evaluate and improve your cyber defenses in a structured way. Military SOCs can better prepare for modern cyber warfare threats and make sure missions are always successful by using mission-focused intelligence, advanced adversary attribution, and operational resilience.

Conclusion

In this paper, we have examined the evolving role of Threat Intelligence (TI) within the context of military cybersecurity operations, particularly focusing on its integration into Security Operations Centers (SOCs). As cyber threats continue to grow in complexity and scale, the need for robust, adaptive defense mechanisms becomes increasingly urgent[13]. The integration of actionable, high-quality threat intelligence is paramount to ensuring that military SOCs are equipped to detect, mitigate, and neutralize cyber threats in real-time, thereby safeguarding critical national security assets.

The research underscores that the traditional models of cybersecurity, while effective in commercial settings, must be adapted for military environments, which face unique challenges such as the protection of classified data, coordination with intelligence agencies, and seamless integration of cyber defense with broader military operations. Through a strategic, tactical, and operational understanding of TI, military SOCs can enhance situational awareness and bolster defensive measures across all branches of the armed forces.

Incorporating Artificial Intelligence (AI) and Machine Learning (ML) into threat intelligence systems provides further advantages[14], enabling faster, more accurate detection of adversarial tactics, techniques, and procedures (TTPs). These technologies allow SOCs to process vast amounts of data and respond more efficiently, reducing response times and improving the overall effectiveness of military cybersecurity defenses.

One of the key findings of this research is the necessity of adapting TI metrics specifically for military environments. Traditional cybersecurity metrics do not adequately capture the operational realities of military cyber defense, necessitating a refined approach to measurement and evaluation. This paper introduced five military-specific SOC metrics designed to address these unique challenges:

---

[13] Sahu, K., Kumar, R., Srivastava, R. K., & Singh, A. K. (2024). Military computing security: Insights and implications. Journal of The Institution of Engineers (India): Series B, 1-25.

[14] Bistron, M., & Piotrowski, Z. (2021). Artificial intelligence applications in military systems and their influence on sense of security of citizens. Electronics, 10(7), 871.

1. **Mission Impact Score (MIS):** Measures the direct impact of cyber threats on mission readiness and operational effectiveness, ensuring that resources are allocated to the most critical threats.
2. **Adversarial Attribution Confidence Index (AACI):** Assesses the accuracy and reliability of identifying threat actors, a crucial factor for strategic military responses and countermeasures.
3. **Cyber-Kinetic Convergence Index (CKCI):** Evaluates the likelihood and severity of cyber threats impacting physical military assets or operations, reinforcing the need for cross-domain security strategies.
4. **Secure Information Exchange Effectiveness (SIEE):** Quantifies the efficiency and security of threat intelligence sharing among military branches, allied forces, and intelligence agencies, fostering a cohesive cyber defense posture.
5. **Operational Resilience Index (ORI):** Measures the ability of a military SOC to maintain operational continuity under sustained cyberattacks, ensuring mission-critical capabilities remain intact during cyber conflicts.

These metrics provide a structured framework for assessing and improving military SOC performance. By focusing on mission-critical impact, adversarial attribution, and operational resilience, military organizations can enhance their cyber defense strategies and maintain superiority in an increasingly contested digital battlefield.

Looking forward, continued advancements in threat intelligence frameworks are critical to maintaining a strategic advantage over adversaries. As cyber warfare becomes more entrenched in modern military conflict, future research should focus on evolving TI metrics, improving predictive analytics, and exploring new technologies like quantum computing for enhanced security. Additionally, fostering greater collaboration between military, government, and private-sector entities will strengthen global cyber defense initiatives, making it more difficult for adversaries to exploit vulnerabilities in critical infrastructure. The growing reliance on AI-driven cybersecurity solutions necessitates ethical considerations and regulatory frameworks to ensure responsible AI implementation within military settings.

References

Ahlm, Eric. ”How to build and operate a modern security operations center.” Gartner Inc (2021).

Ainslie, S., Thompson, D., Maynard, S., Ahmad, A.(2023). Cyber-threat intelligence for security decision-making: A review and research agenda for practice. Computers Security, 132, 103352. https://doi.org/10.1016/j.cose.2023.103352

Alaeifar, P., Pal, S., Jadidi, Z., Hussain, M., Foo, E. (2024). Current approaches and future directions for Cyber Threat Intelligence sharing: A survey. Journal of Information Security and Applications, 83, 103786. https://doi.org/10.1016/j.jisa.2024.103786

Bányász, P., Krasznay, C., & Tóth, A. (2021). A NATO kibervédelmi szakpolitikája. (in Hungarian) in A mai NATO, 130-149.

Bistron, M., & Piotrowski, Z. (2021). Artificial intelligence applications in military systems and their influence on sense of security of citizens. Electronics, 10(7), 871.

Brotby, W. Krag, and Gary Hinson. Pragmatic security metrics: applying metametrics to information security. CRC Press, 2016.

Cyber Strategy Institute. (2025, January 9). Gartner Analysis of Security Operations Centers (SOCs) in 2024 - Understanding the Hype CycleTM for Security. https://cyberstrategyinstitute.com/gartner-analysis-of-securityoperations-centers-socs-in-2024-understanding-the-hypecycle-for-security-operations/

E. Agyepong, Y. Cherdantseva, P. Reinecke and P. Burnap, "Towards a Framework for Measuring the Performance of a Security Operations Center Analyst," 2020 International Conference on Cyber Security and Protection of Digital Services (Cyber Security), Dublin, Ireland, 2020, pp. 1-8, doi:10.1109/CyberSecurity49315.2020.9138872.

Forsberg, J., Frantti, T. (2023). Technical performance metrics of a security operations center. Computers Security, 135, 103529. https://doi.org/10.1016/j.cose.2023.103529

Herrmann, D. S. (2007). Complete guide to security and privacy metrics. In Auerbach Publications eBooks.https://doi.org/10.1201/9781420013283

Kotsias, J., Ahmad, A., & Scheepers, R. (2023). Adopting and integrating cyber-threat intelligence in a commercial organisation. European Journal of Information Systems, 32(1), 35-51.

Dr. Négyesi Imre: DIE VISION DER TRAGBAREN INFORMATIONS-TECHNOLOGIEGERATE; HADMÉRNÖK (1788-1919): 3 4 pp 173-179 (2008)

Négyesi Imre: A megfigyelés és információgyűjtés múltja, jelene és jövője; SZAKMAI SZEMLE (1785-1181): 7 3 pp 35-50 (2009)

Négyesi Imre: TARGBARE UND FELDINFORMATIK-GERATE I.; HADMÉRNÖK (1788-1919): 4 2 pp 333-339 (2009)

Négyesi Imre: TRAGBARE UND FELDINFORMATIK-GERATE II.; HADMÉRNÖK (1788-1919): 4 3 pp 355-362 (2009)

Négyesi Imre: A mesterséges intelligencia és a hadsereg; HADTUDOMÁNY(1215-4121 1588-0605): 29 3 pp 71-79 (2019)

Négyesi Imre: A mesterséges intelligencia katonai felhasználásának társadalmi kérdései; HONVÉDSÉGI SZEMLE (2060-1506 2732-3226): 149 1 pp 133-144 (2021)

Sahu, K., Kumar, R., Srivastava, R. K., & Singh, A. K. (2024). Military computing security: Insights and implications. Journal of The Institution of Engineers (India): Series B, 1-25.

Smeets, M. (2022). No shortcuts: Why states struggle to develop a military cyber-force. Oxford University Press.

Vielberth, M., Bohm, F., Fichtinger, I., Pernul, G. (2020). Security Operations Center: A systematic study and open challenges. IEEE Access, 8, 227756–227779. https://doi.org/10.1109/access.2020.3045514

American Journal of Research, Education and Development
ISSN 2471-9986
2024/3

The potential of cybersecurity exercises in critical infrastructures

Timea Pahi (ORCID: 0000-0001-7346-3450)
Ludovika University of Public Service

Andras Toth (ORCID: 0000-0001-6098-3262)
Ludovika University of Public Service

Abstract

This study examines the potential of cybersecurity exercises that are under the protection of important infrastructure between increasing cyber threats and the adoption of digital systems. This emphasizes the need of regular cybersecurity exercises such as tabletop simulation and the Red Team – Blue Team drilled to evaluate the event response plans, identify weaknesses and improve emergency capabilities. Cooperation between public and private sectors and international partners is essential for effective cyber security. While there are obstacles including modernization and wealth, ongoing enhancement is imperative to increase the flexibility of critical infrastructure and to ensure social and economic stability. Regular cybersecurity exercises optimize defense strategies, strengthen decision-making, and foster a robust cybersecurity culture on organizational and international scales, which is crucial for future protection.

Keywords: cyber exercises, critical infrastructures, incident management, simulations, collaboration

1. Introduction

Cybersecurity exercises serve to enhance the preparedness of critical infrastructures for potential cyberattacks. Essential systems, including energy, water, transportation, and healthcare, increasingly rely on digital technologies, rendering them more susceptible to threats. Consequently, implementing robust cybersecurity measures is imperative to safeguard public safety and national security. These exercises replicate real cyberattacks, allowing organizations to assess their incident response plans and strengthen cybersecurity protocols. Participation allows organizations to identify vulnerabilities, enhance response capabilities, and foster stakeholder collaboration. Various formats, such as tabletop exercises and full-scale simulations, assist organizations in effectively navigating the complexities associated with cyber-attacks. Given the escalating complexity and frequency of cyber-attacks, regular cybersecurity exercises are vital as part of a comprehensive risk management strategy. Such exercises promote a proactive approach to risk mitigation and facilitate compliance with regulatory requirements. Furthermore, collaboration between public and private sector entities is essential for maximizing the effectiveness of these exercises and bolstering the security of

interconnected systems. Despite their advantages, implementing cybersecurity exercises within critical infrastructures faces several challenges. Outdated systems and the intricacy of interdependencies across different sectors complicate protection efforts. Additionally, engaging participants and securing adequate funding can prove challenging. Nevertheless, the continuous enhancement of cybersecurity exercises is crucial for defending against emerging threats and ensuring the resilience of essential services vital to modern society.[1]

The research primarily investigates the following questions, which provide a comprehensive understanding of how cybersecurity exercises protect critical infrastructure, identify and manage vulnerabilities, and enhance collaboration among organizations to ensure effective cybersecurity measures.

1. What is the effect of cybersecurity exercises on critical infrastructure security?
2. How do these exercises facilitate the testing of incident management plans, the identification of vulnerabilities, and the development of response strategies?
3. What diverse methods (e.g., Red Team–Blue Team, Purple Team, tabletop exercises, automated attack simulations) are available for implementing cybersecurity exercises?
4. How do these exercises promote collaboration and communication among critical infrastructure entities, public and private organizations, and international partners?

Grammarly software was employed to systematically enhance the manuscript's grammatical accuracy and clarity. This tool was utilized to identify and correct grammatical errors, ensuring that the text adheres to high standards of written communication.

2. Overview of Critical Infrastructures

Critical infrastructure encompasses those fundamental systems and assets that are indispensable for the functioning of society, the economy, and government. These infrastructures support various sectors, including energy supply, water supply, transportation networks, and healthcare facilities, which form the backbone of modern civilization. Disruption, degradation, or destruction of these key elements can significantly impact public safety, economic stability, and national security.[2]

The critical infrastructure sectors are closely interdependent, with many often relying on each other's operations. For instance, the water management sector is tightly interconnected with the energy sector, which provides the energy necessary to operate water purification and distribution systems. Similarly, transportation depends on energy and communication networks to function efficiently. This mutual interconnection complicates the protection of critical infrastructures, as a vulnerability in one sector can generate risks in several other areas. As critical infrastructures increasingly integrate digital technologies into their operations, the importance of cybersecurity has dramatically increased.[3] The integration of operational technologies and industrial control systems in these sectors targets them for cyberattacks. Cybersecurity measures are essential to safeguard the

integrity and reliability of these infrastructures, particularly in healthcare, transportation, and water management, where system disruptions can have severe consequences for public health and safety.[4]

3. Cybersecurity Exercises

Cybersecurity exercises play a key role in enhancing the preparedness and responsiveness of organizations, especially those managing critical infrastructure. These exercises simulate real cyber threats, enabling organizations to test their incident response plans and identify areas within their cybersecurity strategies that require improvement. Cybersecurity exercises, such as tabletop exercises and full-scale simulations, can take various forms. Tabletop exercises typically focus on discussion-based scenarios, where participants work through decision-making processes and communication strategies under pressure during a simulated cyber-attack. In contrast, full-scale simulations employ a more dynamic approach, mimicking the chaos of an actual cyber-attack and allowing teams to practice their response actions in a controlled environment.[5]

3.1. Goals and Benefits

The primary goal of cybersecurity exercises is to strengthen organizations' resilience to a wide range of cyber threats while providing valuable learning opportunities through simulated crisis situations that emulate real-world challenges.

- **Advanced Response Capabilities:** Participants engage in realistic scenarios that simulate severe security incidents. This hands-on experience equips them with the skills to detect anomalies effectively, manage incidents, and recover critical data systems. As a result, organizations can significantly enhance their incident response protocols and capacity to minimize damage during actual cyber incidents.
- **Identification of Vulnerabilities:** Cybersecurity exercises are pivotal for organizations to uncover potential weaknesses inherent in their systems, processes, and organizational policies. By conducting thorough assessments during these exercises, organizations can identify gaps in their defenses and implement targeted improvements, ultimately fortifying their overall cybersecurity posture against evolving threats.
- **Optimization of Resource Allocation:** These exercises systematically highlight organizational areas that require additional resources or strategic attention. By analyzing the outcomes and findings from the drills, organizations can make informed decisions regarding budget allocation, ensuring that financial resources are directed toward the most critical areas of need, thus enhancing overall operational efficiency.
- **Enhanced Collaboration:** The exercises foster cooperation among diverse organizations and departments within a sector and between various sectors and external partners. This collaborative approach enhances communication and trust and creates a unified strategy for addressing cybersecurity challenges. By working together, entities can share best practices

and resources, leading to greater collective preparedness and resilience of critical infrastructures against cyber threats.[6]

4. The Significance of Cybersecurity Exercises for Critical Infrastructures

Cybersecurity exercises play a key role in increasing the resilience of critical infrastructures against cyber-attacks. These exercises are designed to improve organizations' preparedness and response capabilities in the event of severe security incidents, thereby effectively reducing the impact of cyber-attacks. By simulating crisis situations, organizations can identify vulnerabilities and weaknesses in their operations, fostering the development of a proactive risk management culture. One fundamental factor in successful cybersecurity exercises is the collaboration and information sharing among various stakeholders – governmental agencies, companies, and international partners. This cooperation enables the sharing of best cyber defense exercises and threat intelligence, thereby maximizing the effectiveness of the exercises.

4.1. The Goals and Advantages of Cyber Exercises

Cybersecurity exercises are essential for enhancing the security of critical infrastructures against increasingly sophisticated cyber threats. These structured simulations enable organizations to evaluate and improve their incident response and recovery capabilities rigorously by recreating realistic scenarios that expose vulnerabilities within their processes and systems. This proactive approach facilitates the identification of weaknesses, allowing for timely corrective actions that significantly bolster overall security. Additionally, these exercises foster collaboration among diverse stakeholders, including government agencies, private sector entities, and international partners. Such cooperation enhances a collective understanding of cybersecurity challenges and reinforces contingency plans to ensure that essential functions remain operational during crises. Cybersecurity exercise participation provides valuable insights into supplier relationships and the specific security requirements necessary for effective risk management. This engagement contributes to the establishment of a robust cybersecurity ecosystem. By actively participating in these simulations, organizations fulfill regulatory compliance obligations and position themselves to effectively address future cyber challenges, ultimately safeguarding the integrity of critical infrastructures.

4.2. Best Practices

4.2.1. Developing Realistic Scenarios

To significantly enhance the effectiveness of cybersecurity exercises, critical infrastructure organizations should prioritize the creation of realistic and meticulously crafted scenarios that are intricately linked to their specific operational environments. This process involves the development of scenarios that authentically simulate potential threats to the organization's processes and key assets, such as data systems, communication networks, and physical infrastructure. The Cyber Management Alliance experts stress the importance of exercise developers having in-depth

discussions with key representatives from different organization sectors. This collaborative approach ensures that the scenarios are relevant and relatable, leading to a higher level of participant engagement and a more meaningful learning experience. Specific elements to consider when developing these scenarios include current threat landscapes, historical incidents, and vulnerabilities unique to the organization.[7]

4.2.2. Selecting Appropriate Stakeholders

The overall success and impact of a cybersecurity tabletop exercise are largely influenced by the diversity and representation of its participants. Critical infrastructure organizations must take great care in selecting representatives from a wide range of departments – such as IT, operations, human resources, and legal – as well as different hierarchical levels, from frontline employees to executive leadership. This diverse representation provides a holistic view of the organization's cybersecurity preparedness and fosters an environment where multiple perspectives can be shared. It helps identify communication gaps between departments and highlights areas where coordination and collaboration could be improved. Furthermore, including participants from different functional areas encourages innovative problem-solving and elevates the collective understanding of the organization's cybersecurity posture.[8]

4.2.3. Regular Scheduling of Exercises

Establishing a consistent schedule for cybersecurity exercises – ideally quarterly or semi-annual – plays a pivotal role in preparing participants for the heightened stress and potential disruptions experienced during cyber crises. Regular practice reinforces participants' understanding of protocols and procedures and systematically uncovers opportunities for the critical infrastructure organization to refine and enhance its incident management plans. These exercises help teams respond swiftly and effectively when faced with actual threats by simulating real-world scenarios and fostering a culture of preparedness.

4.2.4. Expert Facilitation

The designation of a qualified expert is fundamental to the success of any cybersecurity exercise. This expert should possess a strong foundation of technical knowledge and excellent interpersonal skills, enabling them to navigate the complexities of the exercise effectively. They are responsible for guiding participants through the scenarios, introducing unexpected challenges to mimic real-life situations, and maintaining high levels of engagement throughout the process. An

experienced expert can also provide valuable insights and context, helping participants better understand the intricacies of the threats faced while enhancing the overall realism of the exercise. Their role is instrumental in ensuring that participants emerge from the exercise with actionable knowledge and practical skills that can be applied in future scenarios.

4.2.5. Comprehensive Documentation

Meticulous documentation of the exercise is crucial for assessing performance and identifying areas that need improvement. This process should encompass detailed records of participants' responses, feedback, and the expert's observations throughout the exercise. Collecting and analyzing this data post-exercise is essential for extracting meaningful lessons and insights, which can inform and advance the critical infrastructure organization's cybersecurity strategy. A well-documented exercise serves as a reflective tool for participants and a strategic resource for leadership, helping to shape a more resilient and proactive cybersecurity posture.[9]

4.2.6. Focus on Improvement

Cybersecurity exercises serve as testing grounds for existing response plans and critical tools for identifying and addressing any weaknesses or gaps within these plans. By conducting thorough evaluations, these exercises can uncover deficiencies in leadership structures, recovery processes, and documentation procedures. This insight is invaluable for critical infrastructure organizations, enabling them to implement targeted improvements and bolster their preparedness for real-world cyber incidents. By systematically revising response plans based on these findings, organizations can enhance their resilience to cyber threats.

4.2.7. Enhancing Collaboration

Fostering collaboration – within and with external partners – is a fundamental best practice for effective cybersecurity management. Engaging in joint exercises with service providers, third-party vendors, and relevant stakeholders can yield a comprehensive understanding of dependencies, workflow integrations, and the specific security requirements of shared data. This collaborative framework allows organizations to more effectively allocate resources to mitigate identified vulnerabilities, ensure compliance with security standards, and enhance the collective cybersecurity posture. Moreover, such partnerships can lead to sharing best practices and innovations, creating a more robust defense against evolving threats.[10]

4.2.8. Measuring Success

To guarantee that cybersecurity exercises result in meaningful and actionable outcomes, critical infrastructure organizations must establish clear and quantifiable metrics for performance evaluation. Key performance indicators (KPIs) such as response times to incidents, the effectiveness of incident management protocols, and the preparedness levels of response teams should be assessed during these exercises. This rigorous analysis provides critical insights into the organization's readiness to confront cyber threats and highlights areas for future training and development. By continuously refining these metrics, organizations can ensure that their cybersecurity strategies remain relevant and effective in an ever-changing threat landscape.[11]

5. Research

The research comprehensively analyzed different cybersecurity exercises, evaluating their measurable outcomes and effectiveness on the critical infrastructures outlined in the NIS2 Directive. This evaluation aimed to identify the potential impact of each practice, focusing on achievable results that contribute to the resilience and security of these essential systems. By categorizing each type of cybersecurity exercise, the study sought to provide a clearer understanding of how they can mitigate risks and enhance the overall stability of critical infrastructure. The NIS2 Directive defines the following critical infrastructure sectors:

1. Energy
2. Transport
3. Banking
4. Financial market infrastructures
5. Health
6. Drinking water
7. Waste water
8. Digital infrastructure
9. ICT service management (business-to-business)
10. Public administration
11. Space[12]

5.1. Types of Cybersecurity Exercises

Organizations can employ various cybersecurity exercises tailored to specific objectives to effectively protect critical infrastructures, such as simulating cyber-attacks, evaluating defensive responses, or optimizing incident management procedures. The following categories of cybersecurity exercises have consistently demonstrated their effectiveness in enhancing the security posture of critical infrastructures.

5.1.1. Red Team – Blue Team Exercises

- **Purpose:** This exercise features a dynamic, real-time simulation between two distinct teams: the Red Team, acting as the attackers, and the Blue Team, serving as the defenders. The primary aim is to rigorously assess and enhance defensive capabilities, response times, and overall readiness against actual cyber threats.
- **Advantages:** These exercises enable organizations to identify and expose security vulnerabilities within their systems by modelling realistic attack scenarios. Participants gain invaluable insights into potential adversaries' tactics, techniques, and procedures, allowing for a more proactive approach to cybersecurity.
- **Recommended for:** IT security teams, personnel in Security Operations Centers (SOC), and professionals in Operational Technology (OT) sectors who are integral to maintaining the security of both IT and operational environments.[13]

5.1.2. Purple Team Exercises

- **Purpose:** This exercise facilitates a collaborative environment where the Red and Blue Teams work together to uncover, analyze, and rectify defensive weaknesses. The focus is on continuous learning and improvement in the organization's cybersecurity capabilities.
- **Advantages:** By integrating the perspectives of both attackers and defenders, Purple Team exercises enhance individual skills and strengthen the organization's overall cybersecurity strategy. This collaborative approach fosters a culture of shared knowledge and encourages implementing best practices for defense against cyber threats.
- **Recommended for:** Organizations seeking to cultivate an adaptive and responsive cybersecurity framework, particularly those prioritizing continuous improvement in attack analysis and defense mechanisms. This exercise is especially beneficial for teams that require ongoing training and development in a rapidly evolving threat landscape.[14]

5.1.3. Red Teaming (Real Attack Simulation)

- **Purpose:** This advanced exercise involves conducting a simulated attack that mimics tactics, techniques, and procedures employed by real-world adversaries. The intent is to bypass the organization's defenses. The aim is to rigorously test the organization's security posture and resilience against sophisticated threats.
- **Advantages:** Red teaming offers insights from the attacker's perspective, allowing organizations to uncover hidden vulnerabilities in their systems, processes, and human factors that may not be apparent in traditional security assessments. These insights are critical for strengthening defensive measures and improving overall cybersecurity strategies.
- **Recommended for:** Organizations with a mature cybersecurity framework seek to challenge their defenses or address specific security concerns, ensuring they are well-prepared for potential real-world attacks.[15]

5.1.4. Automated Attack Simulations (Breach and Attack Simulation – BAS)

- **Purpose:** The primary objective of automated attack simulations is to consistently perform automated penetration tests that evaluate the security posture of a network. These simulations mimic real-world attack scenarios to identify potential vulnerabilities before malicious actors can exploit them.
- **Advantages:** BAS offers the benefits of continuous vulnerability assessment and real-time security checks without requiring manual intervention. This allows organizations to detect

and respond rapidly to emerging threats, ensuring that security measures are always up to date.

- **Recommended for:** This approach is particularly beneficial for large enterprises with complex infrastructures requiring ongoing monitoring and regular testing to maintain a robust security framework.[16]

5.1.5. Tabletop Exercises

- **Purpose:** In this exercise, decision-makers and IT and OT professionals collaborate to navigate a realistic cyberattack scenario. Participants engage in discussions to explore various response strategies, decision-making processes, and the coordination of different departments during a crisis.
- **Advantages:** This method is low-cost and highly effective in assessing and validating the communication pathways and decision-making protocols among team members, allowing for the identification of gaps and areas for improvement.
- **Recommended for:** Top management teams, IT and OT security departments, and incident handlers looking to enhance their preparedness for potential cyber threats.[11]

5.1.6. Incident Response Exercises (Incident Management Testing)

- **Purpose:** This exercise is designed to rigorously assess the reactions of the defending team and the efficacy of their incident management protocols in the face of a real or simulated cyber-attack. Participants respond to scenarios replicating an actual attack's dynamics, evaluating their ability to identify, contain, and remediate incidents.
- **Advantages:** Organizations can significantly reduce detection and response times by conducting these exercises. They also enhance communication and collaboration among key stakeholders, ensuring everyone is aligned during a crisis response.
- **Recommended for:** Security Operations Center (SOC) teams, Incident Response (IR) teams, and executive decision-makers responsible for overseeing cybersecurity initiatives.[17]

5.1.7. Supervisory Control and Data Acquisition and Industrial Control Systems Specific Cybersecurity Exercises

- **Purpose:** Supervisory Control and Data Acquisition (SCADA) and industrial control systems (ICS) specific cybersecurity exercises aim to rigorously test the resilience of ICS and SCADA systems in the face of simulated cyber-attacks. These exercises assess the effectiveness of defense mechanisms and incident response strategies tailored to critical industrial environments.
- **Advantages:** Such exercises provide invaluable insights into the security posture of essential industrial systems, enabling organizations to identify weaknesses in their defense strategies before they can be exploited. They also ensure that personnel are trained to respond effectively to cyber threats, enhancing overall operational resilience.
- **Recommended for:** These exercises are essential for sectors such as energy production, transportation, water management, telecommunications, and other critical infrastructure industries, where system integrity and availability are paramount for public safety and economic stability.[18]

6. Results

The tables below present a comprehensive overview of the measurable and achievable outcomes of implementing various best practices across each critical infrastructure sector. Each table details specific metrics, performance indicators, and benchmarks that illustrate the effectiveness of these practices, enabling stakeholders to assess their impact on overall operational efficiency and resilience within the sector. This information serves as an essential resource for developing robust cyber defense strategies and optimizing operational performance within specific sectors of critical infrastructure. By leveraging this knowledge, organizations can enhance their resilience against cyber threats and ensure the continuous functionality of vital services that support the safety and well-being of the public.

6.1. Energy Sector

Type of Cyber Exercise	Measurable Outcomes	Achievable Outcomes
Red Team – Blue Team Exercise	Conduct a comprehensive assessment of the vulnerability of SCADA and ICS networks, alongside evaluating the effectiveness and robustness of existing defense strategies employed to mitigate potential threats.	Establish protocols to ensure an uninterrupted energy supply while systematically identifying and minimizing potential attack vectors that could compromise system integrity and reliability.
Purple Team Exercise	Thoroughly analyze the overall threat landscape concerning energy networks, focusing on quantifying the threat levels and measuring the response times of various defense mechanisms.	Facilitate quicker threat detection through advanced monitoring systems and foster more effective cooperation between cybersecurity teams and stakeholders, ultimately enhancing the resilience of energy infrastructures.

Red Teaming	Conduct detailed assessments of the energy sector's physical and digital threats, utilizing simulated attack scenarios to reveal vulnerabilities.	Generate actionable insights to develop innovative defense measures and strategies to fortify the electrical grid against current and emerging threats.
Automated Attack Simulations	Systematically identify security vulnerabilities within ICS networks by implementing automated attack simulations that provide real-time data and insights into potential exploitation paths.	Ensure continuous protection of critical systems by integrating advanced threat detection technologies that facilitate immediate response and remediation actions against identified vulnerabilities.
Tabletop Exercise	Evaluate the effectiveness of simulated emergency scenarios, ensuring that roles and responsibilities are clearly defined among participants. Utilize these exercises to identify gaps in response plans and communication processes.	Strengthen the lines of communication and collaboration between power suppliers, regulatory authorities, and emergency response teams, leading to a more coordinated and effective response in real crises.
Incident Response Exercise	Establish benchmarks for detection and mitigation times in response to cyber-attack events, focusing on workflow efficiency and incident reporting structures.	Minimize system downtimes through improved response protocols and develop more effective incident management strategies to enable rapid service restoration following an attack.

SCADA and ICS Specific Exercise	Assess and document specific attack vectors associated with SCADA systems, focusing on software and hardware vulnerabilities that threat actors could exploit.	Develop robust, SCADA-specific defense strategies tailored to industrial control systems' unique operational environment and risk profile, thereby enhancing overall cybersecurity posture.

Table 1: Measurable and achievable outcomes of different cybersecurity exercises in energy sector

6.2. Transport Sector

Type of Exercise	**Measurable Outcomes**	**Achievable Outcomes**
Red Team – Blue Team Exercise	Conduct a comprehensive assessment of vulnerabilities across air, road, rail, and maritime infrastructures by simulating various threat scenarios. This includes identifying weak points in operational protocols, infrastructure integrity, and technological defenses.	Develop enhanced safety measures for transportation systems to prevent potential attacks while implementing strategies significantly reducing detection and response times. The goal is to create resilient systems capable of withstanding and rapidly recovering from disruptions.
Purple Team Exercise	Investigate and analyze potential attacks targeting passenger flow and logistics systems, focusing on understanding the impact of	Formulate and execute faster and more effective response protocols to critical transportation attacks, ensuring that both

	such threats on overall transportation efficiency and passenger safety.	personnel and resources can be mobilized swiftly to mitigate any incidents.
Red Teaming	Identify and document physical and cybersecurity vulnerabilities within rail, air, and sea transportation systems through simulated attacks that test existing security measures	Leverage findings to devise innovative transportation security strategies that address the detected vulnerabilities, thereby bolstering the overall security posture of transportation infrastructures.
Automated Attack Simulations	Conduct in-depth evaluations of the vulnerabilities present in critical transportation systems utilizing automated attack simulation tools to uncover potential weaknesses.	Establish a robust framework for continuous threat monitoring and assessment, enabling proactive identification of emerging threats to the transportation sector and ensuring prompt defensive measures.
Tabletop Exercise	Assess the effectiveness and coordination of emergency communication protocols through realistic scenario-based exercises, examining the flow of information between multiple agencies and stakeholders.	Design and refine crisis management scenarios that provide transportation authorities with a clearer framework for operational response during emergencies, enhancing collaborative decision-making and response times.

Incident Response Exercise	Evaluate the responsiveness and efficiency of digital ticketing systems and control mechanisms during simulated incidents to understand potential failure points and reactivity.	Aim to minimize transportation infrastructure downtime by developing streamlined incident management processes that ensure rapid restoration of services following an event.
SCADA and ICS Specific Exercise	Thoroughly assess the vulnerabilities associated with railway control and air traffic management systems, focusing on integrating technology and human oversight.	Implement enhanced security protocols for both railway and air control systems, ensuring that all critical infrastructure operates under optimal safety and security conditions, thereby protecting public safety and maintaining service continuity.

Table 2: Measurable and achievable outcomes of different cybersecurity exercises in transport sector

6.3. Banking Sector

Type of Exercise	**Measurable Outcomes**	**Achievable Outcomes**
Red Team – Blue Team Exercise	This involves a comprehensive assessment of the vulnerabilities present in digital banking systems and an in-depth analysis of the effectiveness of various phishing techniques used by cybercriminals to target	The ultimate goal is to significantly enhance the protection of sensitive customer information by implementing robust security protocols. Additionally, this process aims to bolster the overall security of banking

	consumers. Metrics such as the number of vulnerabilities identified, the success rate of phishing simulations, and the response times of both teams during testing scenarios are recorded.	transactions, thereby reducing the risk of breaches and unauthorized access.
Purple Team Exercise	This team focuses on quantifying fraud detection rates and analyzing the security response times in real scenarios. By tracking key performance indicators (KPIs) such as the number of fraud incidents detected and the average time taken to respond to these incidents, insights can be gained into current security measures.	The intent is to develop and deploy strategies that lead to faster detection of fraudulent activities. This includes leveraging advanced analytical tools for real-time monitoring, allowing more effective prevention of fraudulent activities before they escalate.
Red Teaming	This process thoroughly analyses the physical and digital threat landscapes that impact banking systems. Banks can gain insights into potential risks by identifying attack vectors and threat actors.	The goal is to fortify customer data protection initiatives by implementing advanced security measures and protocols, ensuring that sensitive information is safeguarded against emerging threats.
Automated Attack Simulations	These simulations identify potential vulnerabilities at banking systems' network and	The objective is to enhance the overall security posture of banking transactions and customer

	application layers. Detailed assessments reveal areas of weakness that cyber attackers could exploit.	data by adopting industry best practices and state-of-the-art technologies designed to provide robust protection mechanisms.
Tabletop Exercise	Conducting mock crisis scenarios allows for evaluating the effectiveness of the bank's crisis communication protocols. Success is measured by participant engagement levels and the clarity of the messages communicated during the exercise.	The primary aim is to enhance the bank's ability to respond swiftly and effectively during financial crises, ensuring that all stakeholders, including customers and employees, are adequately informed and supported.
Incident Response Exercise	These exercises measure critical metrics like the time taken to detect data leaks and the efficiency of security response mechanisms. Detailed logging of incidents and response actions provides a framework for performance evaluation.	The objective is to dramatically speed up the incident response process, thereby minimizing financial losses and reputational damage that can result from security breaches.

Table 3: Measurable and achievable outcomes of different cybersecurity exercises in banking sector

6.4. Financial Market Infrastructures Sector

Type of Exercise	**Measurable Outcomes**	**Achievable Outcomes**
Red Team – Blue Team Exercise	Conduct comprehensive assessments to	Implement strategic measures to enhance

	identify vulnerabilities within stock exchanges and clearing systems. This includes analyzing transactional processes to uncover potential weaknesses malicious actors could exploit.	financial stability, focusing on reducing the risk of fraud and preventing data leakage. This involves developing a robust cybersecurity framework and regularly updating it to adapt to emerging threats.
Purple Team Exercise	Systematically evaluate the effectiveness of current defenses against fraudulent transactions. This includes penetration testing and real-time monitoring to identify gaps in fraud prevention mechanisms.	Advance the capabilities of fraud detection systems by integrating machine learning algorithms and behavior analytics, allowing for smarter, adaptive responses to suspicious activities.
Red Teaming	Identify and assess threats related to network security and potential data leakage incidents. This involves deploying advanced threat intelligence tools to uncover vulnerabilities in financial systems.	Enhance the overall protection of financial systems by applying findings from red teaming exercises to strengthen security measures and refine incident response plans.
Automated Attack Simulations	Initiate automatic vulnerability scanning processes for stock exchange and banking systems. These scans should be comprehensive, covering various attack vectors to	Establish a routine of continuous security testing and protection measures that adapt to the evolving threat landscape. Integration of automated tools can facilitate ongoing assessment and help

	identify weaknesses proactively.	fortify defenses against cyber-attacks.
Tabletop Exercise	Utilize simulated scenarios to assess the effectiveness of financial emergency protocols. This involves engaging key stakeholders in discussions and decision-making processes during crises.	Streamline the execution of financial crisis management strategies to ensure timely responses. Enhancements include refining communication channels and clarifying roles and responsibilities during a crisis.
Incident Response Exercise	Track and analyze response times to cyber incidents, focusing on identifying areas for improvement in the incident management lifecycle.	Implement protocols that promote rapid incident handling, minimize financial losses, and ensure swift recovery from disruptions. This process may involve after-action reviews to learn from incidents and enhance readiness.

Table 4: Measurable and achievable outcomes of different cybersecurity exercises in financial market infrastructures sector

6.5. Health Sector

Type of Exercise	**Measurable Outcomes**	**Achievable Outcomes**
Red Team – Blue Team Exercise	Comprehensive assessment of vulnerabilities within the hospital system, including potential weaknesses	Implementing enhanced cybersecurity measures significantly improving data integrity and confidentiality, resulting in a

	in patient data protection protocols.	stronger defense against ransomware attacks and other cyber threats.
Purple Team Exercise	Thorough evaluation of the healthcare systems' effectiveness in detecting, responding to, and mitigating cyber-attacks.	Development of streamlined incident response strategies that enable faster reaction times, ultimately leading to a notable reduction in patient data breaches and reinforcing trust in healthcare services.
Red Teaming	In-depth analysis of critical medical devices' physical and cyber threat exposure, including vulnerabilities in device software and hardware.	Establishment of robust defense protocols tailored for healthcare devices, ensuring heightened security measures are in place to protect against sophisticated threats.
Automated Attack Simulations	Evaluation of the hospital's defensive capabilities against ransomware through simulated attacks that mimic real-world cyber threats.	Implementation of advanced automated threat detection systems that provide real-time monitoring and proactive protection against potential ransomware infiltration.
Tabletop Exercise	Assessment of the efficacy of emergency response protocols during simulated crisis scenarios	Enhanced coordination and communication among healthcare teams, leading to expedited recovery of medical systems and

	involving various security incidents.	minimizing disruption to patient care during emergencies.
Incident Response Exercise	Detailed tracking of system recovery times following cybersecurity incidents or technical failures within hospital IT infrastructure.	Substantial reduction in system downtime, allowing for uninterrupted patient care services and maintaining the hospital's operational continuity.

Table 5: Measurable and achievable outcomes of different cybersecurity exercises in health sector

6.6. Drinking Water Sector

Type of Exercise	Measurable Outcomes	Achievable Outcomes
Red Team – Blue Team Exercise	Conduct a comprehensive assessment of the vulnerability of water treatment systems, including identifying potential points of failure, and evaluate the manipulability of sensor systems to determine how easily they can be tampered with by malicious actors.	Achieve a significantly safer and more reliable water supply by implementing enhanced security protocols, ultimately minimizing the risks associated with contamination or supply interruptions.
Purple Team Exercise	Thoroughly evaluate the detection time for various types of physical and digital attacks on water infrastructure, including the effectiveness of existing monitoring systems	Develop and implement strategies that facilitate a faster, more efficient response to potential threats, thereby mitigating

	and incident response capabilities.	the impact of attacks before they escalate.
Red Teaming	Perform in-depth assessments to uncover physical and digital vulnerabilities within water supply systems, utilizing simulated attack scenarios to test resilience.	Create and implement innovative defense strategies that bolster the security framework of water supply systems against identified threats.
Automated Attack Simulations	Conduct detailed assessments of network vulnerabilities within water supply systems, utilizing automated tools to simulate potential cyber-attacks and analyze system responses.	Establish routine automated security checks that continuously monitor for vulnerabilities, ensuring that any weaknesses are promptly addressed.
Tabletop Exercise	Simulate crisis management scenarios involving water poisoning or contamination incidents to identify gaps in current response strategies and agency coordination.	Enhance the capability to respond swiftly during disasters, ensuring stakeholders can act decisively to protect public health and restore services effectively.
Incident Response Exercise	Measure and analyze the time required to restore the water supply after an attack, focusing on operational and logistical challenges encountered during recovery.	Reduce the duration of service interruptions significantly so that the community can quickly return to normalcy following an incident.

SCADA and ICS Specific Exercise	Identify specific security vulnerabilities present in SCADA systems used in water treatment processes, focusing on potential weaknesses that attackers could exploit.	Develop tailored defensive measures specific to SCADA systems that enhance their resilience against attacks, ensuring that water treatment operations continue uninterrupted.

Table 6: Measurable and achievable outcomes of different cybersecurity exercises in drinking water sector

6.7. Waste Water Sector

Type of Exercise	**Measurable Outcomes**	**Achievable Outcomes**
Red Team – Blue Team Exercise	Conduct extensive assessments to identify the manipulability of wastewater treatment systems and uncover potential vulnerabilities within control systems. This includes simulating real-world attack scenarios to evaluate the security of operational protocols.	Through these exercises, we aim to enhance the safety and reliability of wastewater treatment processes, ensuring that they function effectively while minimizing environmental damage caused by potential failures or breaches.
Purple Team Exercise	Implement proactive measures to detect and prevent cyber-attacks targeting wastewater treatment facilities, focusing on external threats and insider risks. This involves continuous monitoring and the	Establish a comprehensive incident response strategy that enables quicker and more effective cyber-attack responses, safeguarding water treatment systems' integrity and public health.

	development of advanced threat intelligence.	
Red Teaming	Conduct in-depth evaluations of the physical and digital vulnerabilities of wastewater treatment infrastructure. This includes penetration testing and field assessments to uncover any weaknesses that could be exploited by malicious actors.	Strengthen infrastructure resilience by implementing strategic enhancements and safeguards, resulting in a more secure operational environment.
Automated Attack Simulations	Utilize automated tools to perform comprehensive vulnerability scanning of control systems in wastewater facilities. This involves identifying the latest cyber threats and ensuring that systems are up-to-date with security protocols.	Enhance threat detection capabilities through automation, significantly reducing response times and improving the organization's security posture.
Tabletop Exercise	Design and execute well-structured emergency scenarios that simulate a variety of crises involving wastewater treatment. Participants will engage in role-play to navigate challenges and coordinate responses effectively.	Develop and refine crisis management plans that are effective and actionable, ensuring that all stakeholders are prepared to respond dynamically to emergencies.

Incident Response Exercise	Analyze the recovery time of wastewater treatment systems following various incident types, including cyber-attacks, natural disasters, or operational failures. This involves detailed post-incident reviews and recovery simulations.	Aim for minimal environmental disruption and public health impacts by establishing robust recovery protocols that swiftly restore normal operations.
SCADA and ICS Specific Exercise	Identify and address specific vulnerabilities associated with SCADA and ICS used in wastewater treatment. This includes evaluating system configurations and communication protocols.	Implement targeted security enhancements tailored to SCADA systems, ensuring that they are fortified against potential attacks and capable of maintaining operational integrity under stress.

Table 7: Measurable and achievable outcomes of different cybersecurity exercises in waste water sector

6.8. Digital Infrastructure Sector

Type of Exercise	**Measurable Outcomes**	**Achievable Outcomes**
Red Team – Blue Team Exercise	Comprehensive identification of vulnerabilities across various technology landscapes, including enterprise networks, data centers, cloud computing environments, and IoT (Internet of Things) systems.	Significant enhancement of overall network security frameworks and stronger defenses against Distributed Denial of Service (DDoS) attacks. This approach fosters a proactive security culture within the

	This includes penetration testing and exploitation of weaknesses to assess security postures.	organization, preparing teams for real-world attack scenarios.
Purple Team Exercise	Detailed attack detection rates and average incident response times metrics. This involves analyzing detection tools and methodologies for identifying threats within systems and networks.	Increased precision in threat detection mechanisms and improved synergies among IT security teams, promoting effective communication and collaboration to streamline the incident response process.
Red Teaming	Detailed assessment of vulnerabilities within the digital infrastructure, including application security flaws and architectural weaknesses.	Develop innovative defensive strategies and continuous improvements to protect cloud services and sensitive data in data centers, leading to a more fortified security posture.
Automated Attack Simulations	Real-time automated detection and evaluation of security vulnerabilities across systems, leveraging advanced algorithms and machine learning to identify potential threats continuously.	Establishment of a dynamic and continuous network security monitoring system that allows for rapid adaptation to emerging threats, thereby significantly reducing the risk of breaches.
Tabletop Exercise	In-depth impact analysis concerning the potential outages of mission-critical digital services, which	Formulating a more robust crisis management framework that incorporates lessons learned, enabling

	includes evaluating service dependencies and recovery steps during different cyber incident scenarios.	organizations to execute their incident response strategies efficiently during real cyber-attack situations.
Incident Response Exercise	Thorough evaluation of the organization's capacity to effectively manage data loss and service downtimes. This involves simulating various attack vectors and assessing recovery procedures.	Accelerated incident response times, minimizing data loss and downtime while strengthening the organization's resilience against future attacks.

Table 8: Measurable and achievable outcomes of different cybersecurity exercises in digital infrastructure sector

6.9. ICT Service Management Sector

Type of Exercise	**Measurable Outcomes**	**Achievable Outcomes**
Red Team – Blue Team Exercise	Systematic identification of vulnerabilities within network access points and communication protocols through simulated cyber-attacks and defensive maneuvers. This includes thoroughly analyzing firewall configurations, intrusion detection systems, and data transmission methods.	Establishing a robust framework for secure inter-company information sharing that includes encrypted communication channels, stringent access control policies, and comprehensive data protection strategies to mitigate the risks associated with unauthorized access or data breaches.
Purple Team Exercise	Comprehensive coordination of cybersecurity	Cultivating a collaborative partnership

	defense strategies across various companies to ensure a unified response to cyber threats. This includes regular assessments of threat intelligence sharing and joint defensive operations.	environment that enhances the effectiveness of shared cybersecurity exercises, leading to improved business data protection and a more resilient business ecosystem.
Red Teaming	Evaluation of the effectiveness of cyber-attack strategies targeting both network infrastructure and business relationships, focusing on identifying weaknesses that could be exploited during a real-world attack.	Strengthening cybersecurity defense mechanisms tailored to business collaborations by implementing lessons learned from attack simulations, thus enhancing overall resilience against emerging threats.
Automated Attack Simulations	Executing automated tests to identify and remediate vulnerabilities within inter-company systems, utilizing cutting-edge technologies to monitor threat landscapes continuously.	Development of sophisticated access management and monitoring solutions that ensure real-time detection of anomalies and unauthorized activities, significantly increasing the security posture of inter-company operations.
Tabletop Exercise	Detailed evaluation of the effectiveness and readiness of cybersecurity collaboration with external suppliers and partners through simulated incident scenarios. This	Development of highly responsive incident communication protocols and comprehensive crisis management plans that facilitate timely and effective

	includes assessing communication strategies, decision-making processes, and resource allocation during a cybersecurity incident.	responses to cyber threats across inter-company systems.
Incident Response Exercise	In-depth assessment of data leak detection methods and management capabilities through realistic incident response simulations that test the organization's preparedness for actual breaches.	Improved speed and efficiency of incident response actions, ensuring a swift containment and resolution process in case of data leaks involving business partners, thereby reducing potential damage and recovery time.

Table 9: Measurable and achievable outcomes of different cybersecurity exercises in ICT service management sector

6.10. Public Administration Sector

Type of Exercise	Measurable Outcomes	Achievable Outcomes
Red Team – Blue Team Exercise	Conduct in-depth assessments to identify vulnerabilities in public administration systems and evaluate the susceptibility of government databases to external threats. This includes analyzing potential entry points for cyber attackers and understanding the level of	Implement robust data protection strategies and enhance the safeguarding of sensitive government information by adopting advanced encryption methods, regular security audits, and comprehensive training programs for personnel involved in information management.

	security currently implemented.	
Purple Team Exercise	Systematically evaluating the cybersecurity infrastructure protecting public administration IT systems, including firewalls, intrusion detection systems, and overall network security protocols. Detailed risk assessments will be carried out to quantify potential threats.	To achieve significantly faster cybersecurity response times and more effective incident management protocols. This will include establishing a dedicated cybersecurity incident response team trained to handle various scenarios and deploy corrective measures swiftly.
Red Teaming	Conducting comprehensive simulations of cyber-attacks aimed at causing political and social disturbances, allowing for the identification of critical weaknesses in existing security protocols and emergency response plans.	Strengthening defenses and protective measures for critical state infrastructure, ensuring that essential services, such as energy and transportation, are resilient against potential disruptions.
Automated Attack Simulations	Implementing automated vulnerability assessments for public administration networks and databases. This will involve continuous scanning for weaknesses and real-time reporting of security status.	Establishing a framework for ongoing cybersecurity monitoring that ensures proactive identification of threats and vulnerabilities, thereby enhancing the overall security posture of government systems while

		minimizing the likelihood of successful cyber-attacks.
Tabletop Exercise	Assessing the effectiveness of crisis management plans and communication protocols during simulated cyber crisis scenarios. This includes evaluating team performance, decision-making processes, and inter-agency communication flow.	Developing more efficient strategies for restoring public services in the event of cyber-attacks, leading to quicker recovery times and minimized impact on citizens and stakeholders.
Incident Response Exercise	Evaluating the responsiveness and effectiveness of government systems when faced with cyber threats, measuring how quickly systems can detect, respond, and recover from incidents.	Striving for minimal government service outages during cyber incidents through improved detection systems, rapid response protocols, and redundancy plans to ensure continuous service delivery.

Table 10: Measurable and achievable outcomes of different cybersecurity exercises in public administration sector

6.11. Space Sector

Type of Exercise	Measurable Outcomes	Achievable Outcomes
Red Team – Blue Team Exercise	Conduct comprehensive assessments to determine the vulnerabilities inherent in satellite communication systems,	Implement advanced security protocols to enhance the integrity and safety of satellite data management while ensuring the reliability

	focusing on potential entry points for unauthorized access and targeted attack vectors.	and uninterrupted operation of satellite networks under various threat conditions.
Purple Team Exercise	Thoroughly analyze and identify security threats facing space objects, including satellites and spacecraft, as well as ground control systems that manage and monitor these assets.	Develop and refine rapid cybersecurity response strategies that can be deployed within space infrastructure, enabling quicker identification and neutralization of emerging threats and vulnerabilities.
Red Teaming	Conduct detailed vulnerability assessments targeting space objects (like satellites) and ground stations to uncover weaknesses that could be exploited by malicious actors.	Formulate and implement new, innovative defense strategies and mitigation plans tailored to the specific needs of systems within the space industry, strengthening overall resilience against cyber threats.
Automated Attack Simulations	Introduce cutting-edge automated attack simulations designed to facilitate real-time threat detection across satellite communication and broader space industry networks, employing artificial intelligence to identify anomalies and potential breaches.	Ensure continuous, proactive monitoring of space security infrastructure, maintaining a state of readiness to respond swiftly to detected threats and minimizing potential damage from cyber incidents.

Tabletop Exercise	Foster improved international cooperation and communication among nations during crisis situations involving space assets, ensuring all parties have a clear understanding of roles, responsibilities, and communication protocols.	Establish more efficient risk management frameworks and enhanced coordination mechanisms tailored to satellite systems, facilitating a collaborative approach to mitigating threats and managing incident responses effectively.
Incident Response Exercise	Measure and evaluate the effectiveness of response times to various incidents affecting space technology, including cyberattacks, system failures, and natural disasters.	Achieve a significant reduction in data loss and minimize system downtime in the space industry, thereby maintaining operational continuity and trust in space operations.

Table 11: Measurable and achievable outcomes of different cybersecurity exercises in space sector

7. Conclusions

The article underscores the critical importance of cybersecurity exercises as integral components of securing critical infrastructures against existing and potential cyber threats. These exercises, characterized by meticulous planning, interdisciplinary collaboration, and systematic evaluation, enable organizations to identify vulnerabilities and respond effectively to cyber incidents. Despite challenges such as reliance on outdated technological systems and issues related to funding and stakeholder involvement, a commitment to continuous improvement and the integration of lessons learned from previous experiences can significantly enhance organizational resilience. Incorporating cybersecurity exercises into risk management strategies is imperative to secure modern digital societies amid escalating cyber threats. Furthermore, the article urges policymakers and cybersecurity professionals to prioritize ongoing cyber readiness, collaborative initiatives, and the regular conduct of realistic simulation exercises. Such measures strengthen technological defenses

and ensure compliance with national and international security standards. Ultimately, it is essential to view cybersecurity exercises as a dynamic and ongoing process vital for safeguarding critical infrastructures and ensuring the uninterrupted delivery of essential services.

The conclusions drawn from the analyses clearly show that cybersecurity exercises – various methods such as Red Team, Blue Team, Purple Team, Red Teaming, automated attack simulations, tabletop exercises, incident response exercises, and specialized SCADA/ICS drills – are essential for strengthening the protection of critical infrastructures. These tools not only serve to map out vulnerabilities but also enable the continuous improvement of defensive mechanisms. In the energy sector, the data highlights that potential attack surfaces can be identified by examining SCADA and ICS systems, and response times and the effectiveness of defense strategies can be measured. Based on these measurements, protocols can be developed that ensure supply continuity and system integrity. For instance, the Purple Team exercise focuses on quantifying the threat level and, accordingly, accelerating threat detection. In the transportation sector, the exercises comprehensively examine various modes of transport – air, road, rail, and maritime – mapping physical and digital vulnerabilities. As a result of such tests, weak points that require rapid response can be identified, leading to more effective security measures and crisis management protocols that significantly reduce potential downtime. The exercises in the banking and financial sector are crucial for protecting customer data and preventing fraud. Through Red Team–Blue Team and Purple Team exercises, the failure rates of phishing attempts, the security of transactions, and the speed of fraud defenses can be measured. These results contribute to the continuous strengthening of financial systems and help reduce financial losses while also protecting the infrastructure of the financial market. In the healthcare sector, the exercises primarily aim to protect patient data and ensure the uninterrupted operation of hospital systems. Incident response exercises allow for measuring how quickly systems and staff can react to cyberattacks, thereby reducing data loss and service interruptions. Similarly, tests conducted in managing drinking water and wastewater identify potential vulnerabilities, after which rapid recovery procedures ensure the reliability of public services. Cybersecurity exercises applied in digital infrastructure, ICT service management, public administration, and the space sector particularly reflect the complexity of modern technological systems. For example, automated attack simulations enable continuous, real-time monitoring so that any vulnerabilities can be immediately identified and remedied. Additionally, tabletop exercises facilitate effective communication among various agencies and fine-tune incident management processes, particularly important for protecting critical state systems. The analyses indicate that cybersecurity exercises employ comprehensive,

sector-specific approaches to uncovering vulnerabilities, optimizing defense strategies, and improving incident response times. This regular and targeted training mitigates current risks and promotes continuous development and proactive defense against new threats, ultimately safeguarding the security of society and the economy.

References

[1] S.-T. ROȘCA, "Cybersecurity within critical infrastructures," *Proc. 20th Int. Sci. Conf. "Strategies XXI,"* vol. Technologies – military applications, simulation and resources, 2024, [Online]. Available: https://www.academia.edu/download/116658375/STRATEGIES_XXI_TECHNOLOGIES_MILITARY_APPLICATIONS_SIMULATION_AND_RESOURCES.pdf#page=377

[2] A. Kiss, "Az orosz–ukrán háború hatása a kritikus infrastruktúrákra – fókuszban az energiaszektor," *Hadmérnök*, vol. 19, no. 3, pp. 183–200, 2024, doi: 10.32567/hm.2024.3.11.

[3] P. Bányász, A. Kiss, S. Magyar, and D. Kiss, "Empirical analysis of the cyberattacks of the Russian–Ukrainian war," *Inf. Társad.*, vol. 24, no. 2, p. 9, Aug. 2024, doi: 10.22503/inftars.XXIV.2024.2.1.

[4] A. Toth, "Industrial IoT and 5G in Critical Information Infrastructures," in *Critical Infrastructure Protection in the Light of the Armed Conflicts*, T. A. Kovács, Z. Nyikes, T. Berek, N. Daruka, and L. Tóth, Eds., in Advanced Sciences and Technologies for Security Applications. , Cham: Springer Nature Switzerland, 2024, pp. 173–187. doi: 10.1007/978-3-031-47990-8_16.

[5] K. Kassai, "Emerging Challenges and New Responses, Building Capabilities to Counter Threats in Cyberspace: Questions and Answers on How to Improve Cybersecurity," *Hadmérnök*, vol. 19, no. 1, pp. 121–141, Sep. 2024, doi: 10.32567/hm.2024.1.7.

[6] J. Ebuzor, "Good Governance and Cybersecurity: Enhancing Digital Resilience," in *Advances in Hospitality, Tourism, and the Services Industry*, P. Thealla, V. Nadda, S. Dadwal, L. Oztosun, and G. Cantafio, Eds., IGI Global, 2024, pp. 112–136. doi: 10.4018/979-8-3693-2715-9.ch006.

[7] I. Song, S. Jeon, D. Kim, M. G. Lee, and J. T. Seo, "GENICS: A Framework for Generating Attack Scenarios for Cybersecurity Exercises on Industrial Control Systems," *Appl. Sci.*, vol. 14, no. 2, p. 768, Jan. 2024, doi: 10.3390/app14020768.

[8] N. National Rural Electric Cooperative Association (NRECA), "Improving the Cyber and Physical Security Posture of the Electric Sector (Final Report)," None, 1924082, Mar. 2021. doi: 10.2172/1924082.

[9] A. Grimaldi, J. Ribiollet, P. Nespoli, and J. Garcia-Alfaro, "Toward Next-Generation Cyber Range: A Comparative Study of Training Platforms," in *Computer Security. ESORICS 2023*

International Workshops, vol. 14399, S. Katsikas, H. Abie, S. Ranise, L. Verderame, E. Cambiaso, R. Ugarelli, I. Praça, W. Li, W. Meng, S. Furnell, B. Katt, S. Pirbhulal, A. Shukla, M. Ianni, M. Dalla Preda, K.-K. R. Choo, M. Pupo Correia, A. Abhishta, G. Sileno, M. Alishahi, H. Kalutarage, and N. Yanai, Eds., in Lecture Notes in Computer Science, vol. 14399. , Cham: Springer Nature Switzerland, 2024, pp. 271–290. doi: 10.1007/978-3-031-54129-2_16.

[10] C. Galkaduwa, "Challenges and Opportunities in Information Sharing during Cybersecurity Exercises," Jan. 02, 2024, *Preprints*. doi: 10.36227/techrxiv.170421667.79223854/v1.

[11] N. Chowdhury and V. Gkioulos, "A Framework for Developing Tabletop Cybersecurity Exercises," in *Computer Security. ESORICS 2022 International Workshops*, vol. 13785, S. Katsikas, F. Cuppens, C. Kalloniatis, J. Mylopoulos, F. Pallas, J. Pohle, M. A. Sasse, H. Abie, S. Ranise, L. Verderame, E. Cambiaso, J. Maestre Vidal, M. A. Sotelo Monge, M. Albanese, B. Katt, S. Pirbhulal, and A. Shukla, Eds., in Lecture Notes in Computer Science, vol. 13785. , Cham: Springer International Publishing, 2023, pp. 116–133. doi: 10.1007/978-3-031-25460-4_7.

[12] "Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)." Accessed: Feb. 05, 2025. [Online]. Available: https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng

[13] M. M. Yamin and B. Katt, "Modeling and executing cyber security exercise scenarios in cyber ranges," *Comput. Secur.*, vol. 116, p. 102635, May 2022, doi: 10.1016/j.cose.2022.102635.

[14] L. F. Ilca and T. Balan, "Purple Team Security Assessment of Firmware," in *Online Engineering and Society 4.0: Proceedings of the 18th International Conference on Remote Engineering and Virtual Instrumentation*, Springer Nature, 2021, p. 370.

[15] S. Yulianto, B. Soewito, F. L. Gaol, and A. Kurniawan, "Enhancing cybersecurity resilience through advanced red-teaming exercises and MITRE ATT&CK framework integration: A paradigm shift in cybersecurity assessment," *Cyber Secur. Appl.*, vol. 3, p. 100077, Dec. 2025, doi: 10.1016/j.csa.2024.100077.

[16] M. Brown, "The Evolution of Cybersecurity Testing: Pen Testing, BAS, BAS+, & AEV." Accessed: Feb. 22, 2025. [Online]. Available: https://scythe.io/library/the-evolution-cybersecurity-testing

[17] S. Mases, K. Maennel, M. Toussaint, and V. Rosa, "Success Factors for Designing a Cybersecurity Exercise on the Example of Incident Response," in *2021 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, Vienna, Austria: IEEE, Sep. 2021, pp. 259–268. doi: 10.1109/EuroSPW54576.2021.00033.

[18] D. Kim, S. Jeon, K. Kim, J. Kang, S. Lee, and J. T. Seo, “Guide to developing case-based attack scenarios and establishing defense strategies for cybersecurity exercise in ICS environment,” *J. Supercomput.*, vol. 80, no. 15, pp. 21642–21675, Oct. 2024, doi: 10.1007/s11227-024-06273-9.

American Journal of Research, Education and Development
ISSN 2471-9986
2024/3

Habits that can be acquired during the training and their effects in disaster protection

MUHORAY, Róbert András, Doctoral School of Military Sciencies, PhD student. Email: robert.muhoray@gmail.com. ORCID: 0000-0002-8440-6133

Abstract

Disaster management is a national affair. Training is the fundament for high-quality task performance. Thanks to generational change and technological development, one of the keys tasks of education are to use tools to keep students in the system and give them a perspective on disaster management. Participants in the training acquire and practice the way of thinking, the use of tools and tactics necessary for a successful intervention. The author wants to highlight that the new approaches and practices for different events can contribute students to develop new habits that support following commands, use of tools, teamwork, solving more complex tasks, and tolerating physical trials and exertion, as well as the establishment of a regular working schedule with up to 24-hour shifts.

Keywords: mind programming, disaster management, training, habit, education

Introduction

The main purpose of the disaster prevention is to increase the safety and the sense of security of the general populous and increasing the effectiveness of protection against natural and civilizational disasters, also strengthening the disaster prevention organizational system, as well as increasing the effectiveness of the disaster prevention measures. Disaster management itself is a national priority. [1]

For disaster management workers being able to perform their tasks at a high level, training and education are inevitable. During the training, the students and the staff are present, and they have to step out of their comfort zone. You must have an open mindset to acquire new knowledge and

learn how to apply them. This is not always easy, given that recently gained knowledge may involve some overwriting of the existing habits and approaches.

Formally used habits are the usual, already practiced activities, they are simple, and they offer fast help in practice. However, changing them can have an impact on to the way of one's thinking, just as the approach to individual situations, and the way of solving of tasks too.

In order to achieve outstanding efficiency and the condition of compliance of the VUCA (Volatile, variable, Uncertain, Complex, Ambiguous, uncertain and dynamically changing, even in chaotic situations in which there are mostly a lack of information, and their outcome often cannot be predicted due to the multitude of influencing factors) environment is, that the individual has to formulate expectations and features about himself regarding himself and his desired workstyle.

All these things are greatly contributing to the so-called Peter principle, meaning to overcome limitations, i.e., to become a good leader or commander from an ordinary colleague. Consequently speaking, higher and higher positions require different competences, which was not necessary in the lower ranks. Thanks to this, it can be avoided that someone would be in a position where he/she is unable to properly fulfill, just as the possible development of super-competence, meaning that in the tasks belonged to the position, the success rate is going to be partial, and the rest of the tasks will be incomplete or not going to be completed at all. [2]

However, performance at work can increase, if the challenges and abilities are in the right proportion, i.e., an individual performs in the so called "flow activity". If the challenge given by the task is too high compared to the individual's ability, then he will be anxious, this could trigger an excessive stress response, which can lead to procrastination. And if compared to one's abilities is facing a less of a challenge, then it could lead to boredom and exaggerated routines (superficiality, thoughtlessness). [3]

The fundamentals of changing habits

The brain is a very complicated computer. It is able to process a huge amount of information in a fraction of a second. The storage capacity of the brain is approx. 2.5 petabytes (2.5 million GB). [4] The Nerve impulses operating in the brain have a speed of about 300 km/h. [5] The brain processes 40 million bits of stimulation from the environment per second, from which only 40 bits/second reach

the conscious mind. The rest is stored in the subconscious part of the brain. [6] To process such a large amount of data, the brain needs to be able to automate certain processes. Therefore, it takes less energy to process these operations. Habits are created thanks to automation, and these are practically the "used paths" of the nervous system.

The brain memorizes and records the feelings and actions related to individual thoughts thanks to the connections (synapses) created between nerve cells. The environmental mediated stimulations, and thoughts formulated by authority figures' expectations, they greatly contribute to the formation of a given person's behavioral patterns. These samples are functioning as a program. The programs influence the individual way of thinking. And then thoughts give birth to emotions, emotions lead to actions, which will have results. Therefore, if you have the same or similar thought appears again, thanks to the developed neural connections, our brain goes into "robot pilot" mode, and we automatically perform the action assigned to the thought, even if we are not conscious about the decision and action. [7]

With the help of the mind programming, habit loops can be formed in the brain. Ivan Petrovich Pavlov conducted series of experiments at the end of the 20th century that served and serves as a basis for all those experiments, which are the "training-reward" and the "classical conditioning" method of examining the formation of habits.

The habit consists of the Trigger-Routine-Reward triad, and this is the drive of craving. The trigger is the moment when the brain switches to automatic mode and begins to routinely perform an action. The result of this action will be (among other things) the reward, which is not just a reward in a physical sense, but also in a chemical aspect. In the human body, there are more than 200 hormones, of which dopamine, endorphin, serotonin, and oxytocin are the most important hormones that are responsible for the formation of habits, and they are related to its maintenance too. This is the reward that your body is craving for. The brain hormones continuous desire (craving) for it, that makes him repeat the action associated with habits over and over again, even though the individual recognizes that this action may have a negative effect on him. [8][9]

Behaviors that remain instinctive (due to cultural affiliation and time regardless) are vital. Those approaches, behavior patterns that parents and various authority figures (e.g., teachers, celebrities, friends, gang leaders, whom the individual [child] looks up) can be observed, that most of the time they are imprinted in the subconscious. After being programmed in here, the person's

entire life is determined, unless you become conscious of the recognition and exchange of thought programs. [10] Given that the habit formed by the individual - due to the intensity of the craving - generally speaking, it cannot be easily eliminated, therefore an established habit can only be changed by the simplest way, just by creating it.

So, when the trigger that starts the habit arrives, the individual must be conscious enough to replace the old routine with new one, and start using an action related to a new habit. In other cases, the old custom it easily overwrites the new habit, so the individual returns to the original habit "without noticing" it.

Competencies to be acquired during the training

The personnel and technical conditions are necessary to overcome disaster prevention tasks in existence of a high standard, so as the execution of the procedure, methodology, tool system and the development of training courses. Moreover, these devices are produced in relatively small quantities, therefore, and because of their special design, they are very expensive equipment. Because of the rare occasions, when they can be applied, the training of operators (staff) and the acquired practicing time is in high priority. [11]

The priority goals of human resource development are as follows in the professional disaster management decision-makers' point of view:

- increasing responsiveness, flexibility, and integration,
- appropriate application of personalized motivation based on individual needs,
- as well as providing highly qualified volunteer contributors.

In relation to organizational development, the following requirements appear:

- the development program should fit the disaster prevention strategy,
- the training should focus on factors important to the voluntary organization,
- organizational development should be in line with the organization's strategy and culture sufficiently prepared and planned process. [12]

One of the most important conditions for the effectiveness of disaster prevention operations, is a high-level application of human resources, for which is necessary of the performance of tasks' acquisition of competencies. That is, the continuous provision of training, as well as the maintenance and development of the training itself. This deserves special attention, because to perform the tasks

required to operate the system in any given situation, the most difficult challenge is to replace a trained and prepared specialist. Recent events show that the material and technological needs are much easier to replace than the lost, and not applicable staff.

The Fire Fighting Tactical Regulations and the Technical Rescue Regulations (hereinafter: Regulations) provides that during individual disaster situations (e.g., firefighting, technical rescue), which chain of command is necessary to carry out rescue and damage mitigation, and how to proceed in each case. [12]

Among other things, the Regulations differentiate the procedures related to the following events or define the execution steps related to the events:

- Extinguishing fires in underground structures, rooms, utilities, utility tunnels.
- Extinguishing fires in medium- and high-rise type buildings.
- Extinguishing fires in hall-type structures.
- Extinguishing fires in penal institutions.
- Extinguishing fires in electrical networks and equipment.
- Intervention rules for fires in vehicles.
- Extinguishing fires in vehicles transporting gas, gas pipelines, gas tanks and gas bottles.
- Extinguishing fires in containers storing flammable liquids and their catchment areas.
- Extinguishing fires in oil and gas wells.
- Extinguishing fires in forests and peatlands.
- Firefighting in the presence of dangerous substances.
- Extinguishing fires in radioactive areas.
- Nuclear facilities, nuclear power plants, research reactors, spent nuclear

interventions related to temporary storage of heating elements and their requirements.

The precise and accurate application of these approaches described in the Regulations, is also important, because the development of these rules is based on the decades of experience gathered so far. the risk arising during rescue can be reduced and rescue efficiency can be increased too. All this of course, appear, not only in the performance of firefighting tasks, but also in the case of civil protection.

Civil defense preparation is regulated by § 56 of the Disaster Prevention Act., and it must be organized by point (1). The legislation specifies that the members of the civil defense organization

can be assigned to training and practice (call), the duration of which cannot exceed one year and 40 hours for training, and 72 hours for practice. The objectives of the trainings and system is defined in the National Directorate General of Disaster Management's annual training measures. An important part of the training that the Civil Defense Association supports the training with speakers and specialist materials. The training preferably takes place at the obliger's place of residence, workplace or it must be held in disaster prevention training institution. [13]

However, when someone chooses disaster protection as his profession - could be a volunteer or professional staff - then the change of the way of thinking, and the way of programing is emphasized during the training.

In contrast to civilian life, there is a strong hierarchy and dependency appearance in disaster management. Thanks to this, unconditional obedience to the given orders is expected just as the respect for ranks. Without them, the rescue work could not be carried out properly. Given that the average civilian is mostly not facing disaster situations, he/she will not be able to carry out these preventions professionally, since:

- in a stressful situation, most people freeze or start to panic - shock effect,
- cannot express himself professionally,
- cannot give appropriate instructions,
- does not have the necessary expertise for disaster relief,
- does not know, how:
    - to do reconnaissance,
    - to prepare the intervention,
    - the safety regulations related to the given type of damage event,
    - to ensure intervenors, or
    - to use applicable regulations and rules on himself.

This is also why it is necessary for the students to acquire the formal forms, based on the appropriate foundations during the training - among other things -, greetings and professional expressions, and how to work in a team movement (e.g.: marching) and thinking, also the knowledge of different tools, and procedures, plus the rules.

By changing the way of thinking, new habits can be formed, which thanks to this, the cadets (officer candidates) will be able to think in a team and as a team, in accordance with this, to solve

more complex tasks. They will know the legal environment, they will acquire deployment and tactical knowledge and skills, they will be able to cooperate with several bodies at the same time. Because of the hierarchy, it will be clear to all, that it is a question of responsibility, and it is also possible to maximize the effectiveness of command.

As it also happened during the severe red mud disaster in Kolontár on October 4, 2010, where first the On-Site Operative Tribe and then the Reconstruction Government Coordination Center (here in after: RGCC) operated. It is the task of the RGCC operations management, as well as running the legal, reconstruction and logistics work groups until June 30, 2011. After that the Reconstruction Disaster Prevention Corps with a smaller number of personnel took over the tasks until October 14, 2011, and then Veszprém County Disaster Management The outsourced staff of the Board completed the on-site work by December 31, 2011. [14]

In addition, the more complex task solving procedures and the continuous practice make it possible, that the previously mentioned shock effects can be successfully dealt with by those dealing with disaster management and processing it successfully, so their effects appear to a reduced extent.

Of course, having the necessary knowledge for intervention alone is not enough, since if the commander is not sufficiently careful, the reconnaissance is not adequate, and that time pressure is urgent, then accidents/fatalities may occur during the retreat or even during the rescue, for example, on the occasion of the fire at the shooting range of the University of Technology on August 8, 2006.

Preventing such cases, increasing rescue efficiency, and developing the knowledge base in order to evaluate the work performed, it is the responsibility and duty of the commander. This also requires the preparation of a tactical site plan, which presents how to perform the individual and the group tasks. The site plan also helps to reflect the correctness of the intervention tactical methods. In this way, a written record of all activities remains. The getting to know and the mastering of the preparation of a tactical site plan also already happening during the training. This can provide the commander with a suitable basis to give praise or condemn those involved in the intervention.

In relation to the changes in the way of thinking of the students during the training, they also change their habits/take on new habits on a physical level. These include, among others:

- following command words,
- mastering group training,
- acquisition of forms:

- queuing, formal receptions,
- position formations (rest, be careful),
- salute, gestures (certain),
- execution of movements, turns (whole body),
- endurance of physical trials and loads,
- practicing assembly techniques,
- performing device management, maintenance, and technical services.

Continuous practice of all this helps the students to know the tasks at a skill level and complete them as such. That is, through repetitions, one type of situation becomes a habit solution to the approach, which helps to carry out an effective intervention even when they leave the school desks. On the other hand, the repetitions increase the cadet's tolerance for monotony. And this is also necessary because a completely new lifestyle is needed to be developed, since in civilian life, instead of the general 8-hour working day, it may be 24-hour working hours when they will work in shifts, so the related regularity is also necessary to be mastered.

Education of new generations

In the Middle Ages, the most skillful was the one who could handle the weapon best. Today is the one whose knowledge is in line with the constantly renewing trends, tools, and can keep up with technological development. [15] For this, continuous education, learning, and the educational materials need to be updated constantly.

However, it means difficulty, that, thanks to generational differences, the now growing young people are often more interested in virtual life than in the real world. Most of their lives they spend it on social networking sites and platforms, where they easily make connections, but it's the same going for eliminating them.

The fact, that young people do less memorizing, and they rely on the search on the Internet, causes difficulty and take everything they can find on the internet for granted. As a result, they do not develop a critical attitude and often acquire incorrect knowledge. All this is made more difficult by the fact that young people quickly start to get bored if they don't get one impulse that captures their attention. This leads to a lack of focus.

In the light of these things, education has an increasingly serious task of introducing new methods to apply, which on the one hand helps the acquisition of skills, but also increases the discipline which for the most part, the young people did not receive in their family circle, or it keeps the students in the system and can give them a perspective with which, in the long term, they will be dedicated disaster management officers and deputy officers.

Future research directions

The definition of future research tasks is always an important part of scientific analyses. In my opinion, professional preparation should also include cooperation between implementing organizations involved in disaster management operations, among which cooperation between law enforcement agencies can be highlighted [16]. Equally important scientific aspects may be the foundation for the implementation of the renewed regulation on reliability of critical infrastructures [17, 18], or the use of artificial intelligence tools for preparation purposes [19].

Summary

All activities require learning to perform at a professional level. This can happen empirically and based on theoretical approaches. The goal is for the person to be able to learn new competencies.

It is an integral part of thought programming, that the students learn the traditional (civil) approach, so they already learn the command in the first period of their training action, physical forms, and group movement. A goal is to quit from the former comfort zone and form new habits. Such basic habits are: rule-following, an obedience to orders, team thinking, knowledge of tools, assembly techniques knowledge, intervention and tactical knowledge, precise knowledge of the legal environment.

Whether it is an intervention or an exercise (e.g.: march - reconnaissance – intervention preparation - compliance with safety regulations - intervention - provision of interveners - follow-up works - restoring the original situation), a result can only be achieved if a commander does not work alone, but in cooperation with a team of subordinates they carry out your instructions. In the absence of these, the success of the intervention cannot be guaranteed.

The formation of the new way of thinking is necessary for this, and it begins in firefighter training and during the university education. It becomes a habit through continuous practice, which

habit is not only determines the way of working, but also changes the lifestyle of those who are involved in disaster management.

References

1. CXXVIII of 2011. act on disaster prevention and the amendment of certain related laws, 1. §
2. Peter, Laurence J. – Hull Raymond (1989): The Peter Principle: Why Things Always Go Wrong. Kossuth Publisher, Budapest, pp. 29-56., ISBN: 963-09-3345-4
3. Csíkszentmihályi, Mihály: Flow, The Psychology of Optimal Experience. Akadémiai Publisher, Budapest, pp. 115-228., ISBN 963 05 7770 4
4. Reber, Paul (2010): What Is the Memory Capacity of the Human Brain? Scientific American (May 2010) Download: https://www.scientificamerican.com/article/what-is-the-memory-capacity/ 2021.11.30.
5. Horváth Judit (2016): Light and electron microscopic structure of peripheral nerves (axon, sheaths, terminals). In: Csernus Valér Kállai János, Komoly Sámuel (szerk): Emberi életfolyamatok idegi szabályozása – a neurontól a viselkedésig. Interdiszciplináris tananyag az idegrendszer felépítése, működése és klinikuma témáiban orvostanhallgatók, egészség- és élettudományi képzésben résztvevők számára Magyarországon. Budapest, Pécsi Tudományegyetem; Dialóg Campus Publisher-Nordex Kft., ISBN 978-963-642-631-6, Download: https://regi.tankonyvtar.hu/hu/tartalom/tamop412A/2011-0094_neurologia_hu/ch01s03.html, 2021.04.14.
6. Lipton, Bruce: Rewrite Your MIND (40 Million Bits/Second) | Dr. Bruce Lipton “It Takes 15 Minutes”. https://www.youtube.com/watch?v=eB-vh6VWdcM Download: 2021.05.20.
7. Dispenza, Joe (2019): You are the placebo. Making your mind matter. Budapest, Bioenergetic Publisher, pp. 77-100., ISBN: 978-963-291-355-1
8. Schultz, Wolfram-Apicella, Paul-Ljungbergb, Tomas (1993): Responses of Monkey Dopamine Neurons to Reward and Conditioned Stimuli during Successive Steps of Learning a Delayed Response Task. The Journal of Neuroscience, Year 13/3., pp. 900-913., ISSN 1529-2401

9. Graybiel, Ann - Grafton, Scott (2015). The Striatum: Where Skills and Habits Meet. Cold Spring Harbor perspectives in biology. 7/2015. ISSN: 1943-0264, Download: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4526748/ 2020.11.15.
10. Lipton, Bruce (2006): The Biology of Belief. Budapest, Édesvíz Publisher, pp. 161-169. ISBN 963 528 930 8
11. Vass, Gyula - Zsitnyányi, Attila (2019): The application of multi functional vehicles in disaster management. Military engineer, Year 14/2., pp 45-48.
12. 6/2016. (I. 24.) Instruction of the Ministry of the Interior's National Directorate General of Disaster Management on the issuance of the Fire Fighting Tactical Regulations and the Technical Rescue Regulations
13. Endrődi, István - Jósvai, Attila (2016): Practical Manual - Capacity Development of Voluntary Civil Defense Organizations at the Local Level. Special issue of the Civil Defense Review, pp. 8-11., ISSN 1788-2168
14. Ambrusz, József – Muhoray, Árpád (2015): Eliminating the consequences of the red mud disaster, restoring the damage. Bólyai Review 2015/4. p. 69. ISSN 1416-1443
15. Muhoray, Róbert András (2019): Comparison of Leadership Trainings in Civilian Life and in the Hungarian Defence Forces. Military Science Review, Year 12/4., p. 102
16. Bakai, Kristóf Péter (2012): Bizalom és biztonság. In: Gaál, Gyula; Hautzinger, Zoltán (szerk.) Tanulmányok "A biztonság rendészettudományi dimenziói - változások és hatások" című tudományos konferenciáról: Változások és hatások. Pécs, Magyar Hadtudományi Társaság Határőr Szakosztály Pécsi Szakcsoport pp. 459-462.
17. Mihály, István, László Bérczi, Balázs Bognár, Maxim Kátai-Urbán, Levente Tóth, Lajos Kátai-Urbán, Gyula Vass, and Ferenc Varga. 2025. "Experimental Study to Determine the Leakage Area of Single-Leaf Smoke Control Doors in the Design of Pressure Differential Systems" Fire 8, no. 1: 5. https://doi.org/10.3390/fire8010005
18. Kátai-Urbán Lajos Sibalinné, Fekete Katalin ; Vass, Gyula. Hungarian Regulation on the Protection of Major Accidents Hazards. (2016) *Journal of Environmental Protection, Safety, Education and Management* (2016) 8, 4, 83-86.
19. Tóth, Levente Az intelligens fenyegetés. Hogyan veszélyeztetheti a mesterséges intelligencia a biztonságunkat? Belügyi Szemle, 72 (7). 1187-1205. (2024) https://doi.org/10.38146/bsz-ajia.2024.v72.i7.pp1257-1273

American Journal of Research, Education and Development
ISSN 2471-9986
2024/3

Assessment of Public Security Planning Regulations and Guidlines related to Dangerous Goods Transportation Facilities

Zoltán Csépló PhD, chief inspector, Capital Disaster Management Directorate, Budapest, Hungary, zoltan.cseplo@katved.gov.hu ORCID: 0000-0002-8920-3095

Abstract

The harmful effects of accidents involving dangerous substances on human life and health or on environmental elements that may occur at sites engaged in hazardous activities can be managed using the same system of procedures and technical tools.

In the case of dangerous goods transport facilities, such as road depots, railways stations, combined terminals and ports, the mandatory site and settlement disaster management regulations similar to the major accident prevention regulations exist in a relatively incomplete form. However, chemical accident preparedness activities also require the availability of preventive and preparedness measures introduced by the operators of transport facilities and disaster manament authorities. The availability of prevention, preparedness and response capabilities can be ensured through internal emergency planning activities or by applying public safety planning measures.

In this article, the author will examine in detail the international and domestic public safety regulatory requirements affecting dangerous goods transport facilities. The author's researc objective will be also the overwiev of the main features of the related guidance materials and scientific literature.

Keywords: dangerous goods transportation facilities, public security planning, emergency response planning, major accidents, chemival accident preparedness

Corresponding author:

Zoltán Csépló PhD, chief inspector, Capital Disaster Management Directorate, Budapest, Hungary, zoltan.cseplo@katved.gov.hu ORCID: 0000-0002-8920-3095

1. Introduction

Protection against accidents involving dangerous substances requires the application of prevention, preparation, accident prevention and recovery measures by authorities and operators [1]. In addition, the related risk analysis, emergency planning and prepareddness activities are mostly based on the same procedural and methodological foundations for both accident prevention and recovery. The management and technical requirements governing the chemical accident preparedness activities are fundamentally independent of the cause of the accident events invonving dangerous substances. Accordingly, in terms of technical failure, human error or external causes, accident prevention and restoration activities require the same disaster management legal regulations and the existence of the same organizational and technical conditions for accident prevention [2].

The sites engaged in hazardous activities primarily include establishements dealing with dangerous substances falling under the scope of Chapter IV of Act CXXVIII of 2011 on disaster management dealing with protection against major accidents involving hazardous substances. This also includes sites not falling under the scope of Chapter IV of Disaster Management Act but representing similar industrial safety risks. These sites are the so called dangerous goods transportation facilities falling under the scope of certain transportation laws [3]. The situation is similar with facilities dealing with nuclear and radioactive materials, mining waste storage facilities and dangerous military objects. From the perspective of major accident prevention, such activities also include sites dealing with dangerous

substances that have a resilience planning obligation under Act LXXXIV of 2024 on the resilience of critical organizations [4].

In Hungary, dangerous goods are mainly transported by road and rail. In most cases, the transport route passes through residential areas, in which case the population is at increased risk due to the quality of the dangerous goods transported [5]. In the case of dangerous goods transport facilities, such as road depots, railways stations, combined terminals and ports, the mandatory site and settlement disaster management regulations similar to the major accident prevention regulations exist in a relatively incomplete form. However, chemical accident preparedness activities also require the availability of preventive and preparedness measures introduced by the operators of transport facilities and disaster manament authorities. The availability of prevention, preparedness and response capabilities can be ensured through internal emergency planning activities or by applying public safety planning measures.

The research objective of present study is to analyse in detail the international and domestic public safety regulatory requirements affecting dangerous goods transport facilities. In addition, the present research also includesalso the overwiev of the main features of the related guidance documents for the implementation of legal regulations and also the assessment of specific scientific literature.

2. Evaluation of emergency response planning experiences for dangerous goods transportation facilities

In accordance with my experience, the compliance with chemical accident preparedness requirements can basically be ensured by bringing the sites of these hazardous activities under the scope of Chapter IV. of the Disaster Management Act. This regulatory need has already arisen during the development of the industrial safety institutional system between 2010-2011, but has not been implemented so far. In this legal regulatory situation, the availability of prevention and preparedness capabilities for hazardous goods transport facilities can be ensured from a disaster

management perspective in two regulatory ways, that are the emergency respons planning and the public security plannning regulations.

Chapter VI of the Implementing Decree of the Disaster Management Act (Government Decree 234/2011 (XI. 10.)) regulates the emergency planning requirements. This activity may also extend to dangerous goods transportation facilities, where workplace, settlement and regional emergency response plans may also be prepared, tested and applyed in the event of the occurence of emergency situations [6].

These planning systems determine the general requirements and levels of emergency responce planning, the scope and content of the plans. Annex 2 of the regulation lists hazardous effects, in addition to dangerous establishments falling under the scope of Chapter IV of the Disaster Management Act, including facilities carrying the risk of accidental release of dangerous and the risks of transportation of dangerous goods. However, the content and form requirements for emergency response planning, preparation, practice and application, as well as the detailed rules for implementation, do not reach the regulatory level of establisments falling under the Chapter IV. of Disaster Management Act [7].

The effectiveness of emergency response measures depends significantly on the state of implementation of fire prevention technical requirements [8].

3. Assessment of international and domestic regulations on public security planning for dangerous goods transportation facilities

The system of rules for the transport of dangerous goods by road has been developed by the Economic Commission for Europe, set up by the United Nations Economic and Social Council in 1947, and is constantly adapted to scientific and technical progress. The Convention, entitled the Agreement concerning the International Carriage of Dangerous Goods by Road (hereinafter referred to as ADR), was signed in Geneva on 30 September 1957 and entered into force with its Annexes on 29 January 1968 [9]. The UN ECOSOC Sub-Committee of Experts on the

Transport of Dangerous Goods is working on the development of the "UN Recommendations on the Transport of Dangerous Goods, Model Regulations," which will provide a common basis for the structure of all transport sectors. The amendments to the ADR based on these Model Regulations are drafted by the Working Party on the Transport of Dangerous Goods (RID/ADR/ADN Joint Meeting) of the UN Economic Commission for Europe (UNECE) Inland Transport Committee (ITC) [10].

The introduction of the other preparatory legal institution can be traced back to international and European Union regulatory efforts following the terrorist acts that occurred in the early 2000s. Following the terrorist attacks on the United States on 11 September 2001, the importance of protecting against the misuse of dangerous goods, which are an important part of the flow of goods and the functioning of the economy, was recognised. The UN Economic and Social Council has therefore included provisions in the UN Model Regulations to help prevent terrorist acts. These provisions are uniformly contained in Chapter 1.10 of the Transport of Dangerous Goods Regulations, based on the UN Model Regulations, also known as the "Orange Book" [11].

Security provisions were added to the international regulations on the transport of dangerous goods in 2005. The aim of the new provisions was to prevent unauthorised possession of dangerous goods, in particular their use in terrorist acts. With the inclusion of Chapter 1.10, companies handling dangerous goods presenting a high risk to public safety were required to prepare a public security plans [12].

For about two decades, specialized international organizations in the transportation sector have been trying to solve the uniform application of the provisions of public safety planning legislation with methodological guides. Guidance on the practical implementation and application of ADR Chapter 1.10 has been developed by a panel of industry experts from eleven organizations. The document is entitled "Industry Guidelines for the Security of the Transport of

Dangerous Goods by Road" [13]. The document was first published in April 2005 and last revised in 2016. The Guidelines are not adapted to the changes in the ADR, and the above-mentioned professional body has been working on their update and harmonization since 2013. In addition to not being a mandatory regulation, the guide is not accompanied by any official inspection authority, as a result of which the adequacy, functionality and effectiveness of the public safety plan cannot be clearly ensured [14].

In addition to road transport activities, the obligation to prepare an internal emergency response plan according to RID subchapter 1.11 is a legal obligation only in the case of railway marshalling yards. However, this legal institution is only applied to a specific range of dangerous goods, which is not the same as in the case of major accident prevention regulation.

In the Member States of the European Union, including Hungary, Directive 2008/68/EC on the inland transport of dangerous goods introduced the application of international public security planning regulations for road, rail and inland waterway transportation. In Hungary, legal regulations are established by the biennial transport sector regulation at the government decree level.

However, the provisions of international, European Union and domestic regulations do not include the prevention, preparedness, emergency response and recovery operator requirements applied to establisments dealing with dangerous substances in the Seveso III Directive, nor the industrial safety authority licensing and supervision powers that ensure their application. There is a separate regulation in Hungary for the inspection and application of fines for vehicles and sites transporting dangerous goods.

Professional associations representing companies involved in the production and transport of dangerous goods also contribute independently to the effective practical implementation of public safety regulations 1.10 by preparing professional recommendations and guidelines. One such a document is the European Gas Association's ADR Transport Safety Guide [15]. It can also be said in general that the

efficiency of public safety planning can be increased by increasing the cooperation between law enforcement organizations [16].

Some industrialized countries have issued their own regulatory guidance. One such document is the UK Transport Authority's official recommendation for the road and rail transport sectors [17], which added a risk analysis methodology supplement to the explanatory notes to the UNECE guidelines. The United States Department of Transportation has prepared several methodological enforcement recommendations, an example of which is HMR 49 CFR (171-180) Public Safety Requirements for the Transportation of Dangerous Goods [18], or professional guidelines issued for the safe implementation of shipments related to agricultural products [19].

In the case of the rail transport sector, the *"Guide to the preparation of internal emergency plans at marshalling yards"* was published in 2003 under the auspices of the UIC International Union of Railways [20], which covers railway marshalling yards falling under the scope of Chapter 1.11 of the sectoral regulation.

Of course, the aforementioned guidelines provide assistance in the preparation of internal emergency plans and public security plans, but they do not constitute a legal regulatory obligation and are not accompanied by a provision or procedure granting precise authority provisions. In addition, the content of the guidelines does not meet the emergency planning requirements, thus no uniform and harmonized data is provided for the appropriate level of foundation of chemical accident preparedness measures.

The effective application of emergency response plans requires the identification of the risks of potentially occurring in case of major accidents, the determination of the presonell, equipment and infrastructure necessary for emergency respons organizations of the operators.

4. Introduction to the requirements of the "Industry Guidelines for the Security of the Transport of Dangerous Goods by Road"

The guidance document named as "Industry Guidelines for the Security of the Transport of Dangerous Goods by Road" consists of the main part and four annexes.

The first annex recommends technical solutions for securing temporary storage sites, the second deals with practices for the management of the undertaking and the reduction of public safety risks. The third annex discusses technical solutions to prevent or deter theft of vehicles or cargo during a transport operation and the fourth is a model security plan.

The security plan is divided into five sections: company information, security management, communication, security measures and other information. It can be seen that the document provides detailed recommendations on the planning process and the preparation of the security plan [5].

In the public security plan, information on the company should include the name, full correspondence address and contact details (telephone, e-mail) of the company, the name and contact details (telephone, e-mail) of the appointed security manager and a summary statement of the dangerous goods handled which present a high risk to public security.

The safety management section lists the persons responsible for safety issues and those authorized to handle dangerous goods presenting a high risk to public safety, together with a description of their duties. Procedures for recording safety meetings, receiving and transmitting public safety information to competent personnel, investigating public safety incidents, handling public safety alerts, storing sensitive public safety information and accounting for the movement of dangerous goods involving a high risk to public safety are also described. Also included in this section are details of security equipment, including the maintenance programme and operations to be carried out in the event of equipment failure, and information on the public security awareness training programme [11].

The communication section of the plan includes sections on site-to-vehicle communication links, site public safety alerting, restricted access area designation and vehicle protection.

The last, fifth section of the security plan contains other information. Appendixes A, B, C and D of the plan contain a list of persons responsible for dealing with public safety issues and their duties, a list of persons authorized to handle dangerous goods involving a high risk to public safety, schematic drawings of restricted areas and a chronological record of amendments to the security plan.

The plan should be based on the general situation, not on individual shipments. It is possible that some of the required elements of the plan may already have been prepared to comply with other legal obligations or quality management systems, and these should be referred to.

There are three steps to developing a security plan. The first step is to identify the threat:

- for news and information on current national and international circumstances or terrorist organizations,
- what the police's position is on the possibility of a terrorist act occurring in the area of operation of the organization,
- whether there could be any attractive targets in the facilities or personnel of an organization,
- could be harmed by an attack on a high-risk neighbor? [14]

In the second step, it is necessary to identify the points to be protected and how they are vulnerable to a terrorist attack. The third step is to take measures to reduce the risk to an acceptable level. It is essential that planning and associated responsibilities are the full responsibility of a single person with appropriate authority. The actors in the supply chain should cooperate with each other and with the authorities in the exchange of information on threats, public security measures and response to public security incidents. The main problem for the transport of dangerous goods is the known or predictable movement of vehicles. A particular problem is fuel transport vehicles, which have little separation from public traffic and unauthorized access when discharging fuel [14].

Typically, four types of sites and cargoes can be distinguished on the basis of risk, based on volume, occurrence and importance:

- low-volume or infrequently used, low-priority goods,
- low-priority goods used in large quantities or more frequently,
- small quantities of high-priority goods used in small quantities,
- high volume, high importance goods. [14]

Security planning based on hazard analysis can reduce the consequences of incidents. Safety planning must define the measures to be taken in the event of an accident involving hazardous materials, as well as the human and material resources required to implement them. Special training for personnel involved in security interventions should be part of security planning and tested through practical exercises. Safety plans should be managed as part of the management system and the results incorporated into internal rules. Considering the characteristics of combined terminals, i.e. the fact that the current types and quantities of hazardous materials are constantly changing, the following three effective technical solutions have been proposed for security planning:

1. Water shield: The device is a special push nozzle with a standard Storz clip, usually made of aluminium. A vertical metal plate is connected to the horizontal adjustment tube with a special gap between the metal plate and the tube.
2. Mobile safety bund: The incidence of accidents involving hazardous fuel and the extent of fluid leakage can be reduced by using a safety guard. The material entering the tank can be extracted into an empty tank either by gravity or by a pump.
3. Safety bund connected to an underground collecting system: Hazardous materials can be stored in a separate area, which can also be used as a safety bundle. The concrete base of the storage area is covered with an acid-resistant, chemical-resistant plastic layer. The slope prevents the ingress of potentially hazardous materials and rainwater. enters the drainage opening of the metal grid. [11]

The effectiveness of public security planning measures also depends on the cooperation of authorities, law enforcement agencies and social organizations (voluntary rescue organizations) [21)].

6. Summary and conclusions

In Hungary, as regards the control of the transport of dangerous goods, the presence of the disaster management authorities in all transport sub-sectors will continue to be of paramount importance which will make a major contribution to transport safety and, through this public safety. The transport of dangerous goods is an integral part of the functioning of the economy, and it is impossible to avoid that large quantities of them come into close proximity to the public. The transport of dangerous goods, which carries a high risk to public safety, is encoded in the execution of terrorist acts, and the study of this subject is topical and of great importance. The dangerous goods transport sector and the authorities have the task of developing and operating procedures to protect both the material and the external environment. Besides the risk of accidents the possibility of misuse can be a real danger again.

The regulation of the transport of dangerous goods must protect both the material and the environment. In planning the delivery of goods to their intended destination in a timely and safe manner, the risk of accidents must be considered as well as the possibility of misuse, and the transport of dangerous goods is coded into the execution of terrorist acts. It should be borne in mind that the practical application of the law and the necessary partial regulation need to be assessed in the light of the challenges of the security environment. Together, the safety audits of the dangerous goods safety adviser, the safety of the operation of the means of transport, the content of the security plan and risk analysis are the basis for preventing the misuse of dangerous goods.

References:

[1] Kátai-Urbán Lajos Sibalinné, Fekete Katalin ; Vass, Gyula. Hungarian Regulation on the Protection of Major Accidents Hazards. (2016) Journal of Environmental Protection, Safety, Education and Management (2016) 8, 4, 83-86.

[2] Kátai-Urbán, Maxim ; Érces, Gergő ; Vass, Gyula ; Cimer, Zsolt: Veszélyes áru raktározás oltóvízszennyezéssel kapcsolatos tűzvédelmi követelményeinek értékelése. Polgári Védelmi Szemle 16 : különszám pp. 312-323. (2024)

[3] Bleszity, János; Kátai-Urbán, Lajos: Подготовка специалистов в области промышленной безопасности в Венгрии. Pozhary i Chrezvychajnye Situacii: Predotvrashenie Likvidacia 11: 2 pp. 53-58. (2014)

[4] Bognár, B. 2023. Social Resilience "Security Is What We Do!" Védelem tudomány 7(2) 49-64.

[5] Almási, Csaba; Vass, Gyula; Kóródi, Gyula; Kátai-Urbán, Lajos. Security Planning in the Transport of Dangerous Goods by Road. American Journal of Research Education and Development 2023: 4 pp. 4-13. (2023)

[6] Szakál Béla Cimer, Zsolt ; Kátai-Urbán, Lajos ; Vass, Gyula: Veszélyes anyagokkal kapcsolatos balesetek elleni védekezés I.: módszertani szakkönyv veszélyes anyagok és súlyos baleseteik az iparban és a közlekedésben. Budapest, Korytrade (2015)

[7] Berger, Ádám, Lajos Kátai-Urbán, Zsolt Németh, Attila Zsitnyányi, Maxim Kátai-Urbán, and Zsolt Cimer. 2024. "Applicability of Design Methodology for the Remediation Bund of Flammable Dangerous Liquid Storage Tanks" Fire 7, no. 7: 246. https://doi.org/10.3390/fire7070246

[8] Mihály, István, László Bérczi, Balázs Bognár, Maxim Kátai-Urbán, Levente Tóth, Lajos Kátai-Urbán, Gyula Vass, and Ferenc Varga. 2025. "Experimental Study to Determine the Leakage Area of Single-Leaf Smoke Control Doors in the Design of Pressure Differential Systems" Fire 8, no. 1: 5. https://doi.org/10.3390/fire8010005

[9] Almási, Csaba; Kátai-Urbán, Lajos; Vass, Gyula: Ipari és közlekedési balesetek okainak vizsgálata, különös tekintettel a természeti katasztrófák hatásaira. In: Bodnár, László; Heizler, György (szerk.) Konferenciakiadvány: Természeti Katasztrófák Csökkentésének Világnapja Nemzetközi Tudományos Konferencia. Budapest, RSOE (2021) 369 p. pp. 251-266.

[10] Almási, Csaba; Cimer, Zsolt; Kátai-Urbán, Lajos. Mezőgazdasági felhasználású veszélyes áruk közúti szállítási tapasztalatai - 1. rész. Védelem Tudomány: 5 : 2 pp. 118-136. (2020)

[11] Almási, Csaba; Christián, László; Kátai-Urbán, Lajos; Vass, Gyula: Security Planning in Transport of Dangerous Goods by Road in Hungary. In: Michal, Titko; Erika, Mošková; Katarína, Košútová (szerk.) Riešenie Krízových Situácií v Špecifickom Prostredí : zborník príspevkov z 25. vedeckej konferencie s medzinárodnou účasťou. Zilina, Szlovákia: Žilinská univerzita v Žiline (2022) 150 p. pp. 12-18.

[12] Almási, Csaba; Kátai-Urbán, Lajos; Cimer, Zsolt: ABV-felderítő eszközök bemutatása és fejlesztési lehetőségei. Védelem Tudomány 8 : különszám pp. 195-205. (2023)

[13] UN ECE 2016. ENSZ Európai Gazdasági Bizottság. Közbiztonsági irányelvek a közúti veszélyes áru szállításhoz („Industry Guidelines for the Security of the Transport of Dangerous Goods by Road"), Geneva, Switzerland

[14] Almási, Csaba; Cimer, Zsolt ; Kátai-Urbán, Lajos ; Vass, Gyula: Prevention of Terrorist Attacks during the Transport of Dangerous Goods by Road in Hungary. American Journal of Research Education and Development 2022 (2) 2-10. (2022)

[15] European Industrial Gases Association, 2020. ADR Transport Security Guidelines. Online: https://www.eiga.eu/?s=ADR+TRANSPORT+SECURITY+GUIDELINES (downloaded: 10.09.2024.)

[16] Bakai, Kristóf Péter (2012): Bizalom és biztonság. In: Gaál, Gyula; Hautzinger, Zoltán (szerk.) Tanulmányok "A biztonság rendészettudományi dimenziói

- változások és hatások" című tudományos konferenciáról: Változások és hatások. Pécs, Magyar Hadtudományi Társaság Határőr Szakosztály Pécsi Szakcsoport pp. 459-462.

[17] GOV UK Department for Transport, 2025.Security requirements for moving dangerous goods by road and rail. Online: https://www.gov.uk/government/publications/security-requirements-for-moving-dangerous-goods-by-road-and-rail (downloaded: 10.09.2024.)

[18] U.S. DOT, 2023. Pipeline and Hazardous Materials Safety Administration. Security Requirements Brochure. Online: https://www.phmsa.dot.gov/training/hazmat/security-requirements-brochure (downloaded: 10.09.2024.)

[19] U.S. DOT, 2023. Pipeline and Hazardous Materials Safety Administration. Transporting Agricultural Products Safely. Online: https://www.phmsa.dot.gov/training/hazmat/transporting-agricultural-products-safely (downloaded: 10.09.2024.)

[20] UIC 2003. Nemzetközi Vasútegylet „Útmutató a belső veszélyelhárítási tervek készítésére a rendezőpályaudvarokon" c. döntvénye, (International Railway Association, decision "Guideline for the preparation of internal emergency plans at marshalling yards")

[21] Bakai Kristóf Péter: A Budapest Önkéntes Mentőszervezet megalakulása és működésének első tíz éve. Polgári Védelmi Szemle XVII.: 2025 Különszám pp. 42-54. (2025)

ISSN 7234561-6