A CONCEPTUAL THREE-TIER MODEL FOR MANAGING UNCONVENTIONAL TERRORIST RISKS TO CRITICAL INFRASTRUCTURE IN THE EUROPEAN UNION

Ondřej Vozňák*

Abstract

Unconventional terrorist threats, including cyberattacks, hybrid operations, and the misuse of unmanned aerial systems, are fundamentally reshaping the security environment of critical infrastructure in Europe. Existing risk-management approaches remain largely sector-specific and reactive, limiting their effectiveness in addressing complex, multi-domain, and low-probability high-impact threats.

The aim of this article is to develop and conceptually justify a three-tier risk-management model for unconventional terrorist threats to critical infrastructure in the European Union. The study adopts a conceptual and analytical approach based on a targeted literature review and comparative policy analysis of European and international frameworks.

The article identifies key limitations of current approaches, particularly their fragmentation, insufficient integration of economic and security dimensions, and limited capacity to address systemic and cascading risks. In response, it proposes a structured model based on three interconnected layers: prediction, prevention, and resilience.

The findings suggest that a multi-layered and adaptive framework can enhance anticipatory decision-making, reduce vulnerabilities, and improve recovery capacities, thereby contributing to both security and economic stability. The model also highlights the importance of cross-sector coordination and governance integration in the EU context. While the framework remains conceptual, it provides a foundation for further empirical research and practical application in critical infrastructure protection.

Keywords

Critical infrastructure; unconventional terrorism; risk management; hybrid threats; resilience; European Union

Introduction

Unconventional terrorist attacks are fundamentally reshaping the contemporary security environment by targeting not only the physical components of critical infrastructure but increasingly exploiting hybrid, technologically advanced, and multi-domain strategies to disrupt societal and economic systems. While traditional forms of terrorism relied predominantly on kinetic violence, current threat vectors combine cyberattacks, unmanned aerial systems, disinformation

* PhDr. Ing. et Mgr. Ondřej Vozňák, MSc. Masaryk University, Faculty of Social Studies, Brno, Czech Republic; University of Hradec Králové, Faculty of Arts, Hradec Králové, Czech Republic

campaigns, and insider-enabled operations capable of generating cascading and systemic disruptions across interconnected infrastructures [1]. Due to its high level of interdependence and its central role in ensuring essential services, critical infrastructure has become particularly vulnerable to such complex threat configurations, where localized disruptions can rapidly escalate into broader regional or transnational crises [2]. Existing research highlights that cyber and hybrid threats are especially effective in circumventing conventional protective measures, exposing structural weaknesses in current security paradigms designed primarily for more predictable and sector-specific risks [3]. Moreover, processes such as digitalization, infrastructural interconnectivity, and system aging further amplify these vulnerabilities, contributing to what has been described as a "new normal" of persistent and evolving security risks [4].

Despite the growing body of literature addressing critical infrastructure protection, existing approaches tend to remain fragmented, often focusing on specific threat domains such as cybersecurity, hybrid warfare, or physical protection in isolation. Similarly, economic implications of infrastructure disruption are frequently analysed separately from security considerations, while decision-making frameworks for risk management are typically developed without fully integrating the complexity of unconventional, low-probability but high-impact threat scenarios. This fragmentation creates a significant research gap, particularly in the European context, where critical infrastructure governance requires coordinated, cross-sectoral, and multi-level approaches that reflect both security and economic dimensions of risk.

The aim of this article is to develop and conceptually justify a three-tier risk-management model for unconventional terrorist threats to critical infrastructure in the European context. The proposed model is designed to integrate predictive, preventive, and resilience-oriented components into a coherent analytical framework capable of addressing the dynamic and uncertain nature of contemporary threats. To achieve this aim, the article addresses the following research questions:

1. What categories of unconventional terrorist threats most significantly challenge existing critical infrastructure protection frameworks?
2. What are the principal shortcomings of current risk-management approaches in the European Union in addressing such threats?
3. How can a three-tier model based on prediction, prevention, and resilience enhance strategic risk management of critical infrastructure?

The contribution of the article lies in integrating security and economic perspectives into a structured conceptual framework that reflects the interdependencies of modern critical infrastructure systems. Rather than proposing a purely sectoral or reactive approach, the article advances a holistic and adaptive model that supports decision-making under conditions of uncertainty and limited empirical data. By doing so, it provides a foundation for further operationalization and empirical testing of risk-management strategies in the context of unconventional terrorist threats.

Recent scholarship and policy development increasingly conceptualize critical infrastructure as a complex and highly interconnected socio-technical system exposed to converging physical, cyber, informational, and organizational threats. In the European context, this shift is reflected in the adoption of Directive (EU) 2022/2557 [1] on the resilience of critical entities and Directive (EU) 2022/2555 (NIS2) [2], both of which move beyond earlier sector-bound protection approaches toward a broader resilience-oriented framework emphasizing risk management, preparedness, incident reporting, and cross-sectoral coordination [1][2]. At the strategic level, international organizations such as the OECD and NATO stress that critical infrastructure resilience must be understood as a systemic governance challenge requiring coordination across sectors and jurisdictions, particularly in the context of digitalization, geopolitical instability, and increasing interdependencies [3][4].

Recent academic literature further advances this perspective by emphasizing the multi-domain nature of contemporary threats. Research on hybrid threats demonstrates that modern hostile activities increasingly combine cyber operations, disinformation campaigns, economic coercion, and physical disruption in ways that deliberately exploit systemic vulnerabilities and blur the boundaries between peace and conflict [5][6]. Parallel developments in the study of cyber-physical systems highlight that critical infrastructure must be analysed as an integrated system in which disruptions can propagate across digital and physical layers, producing cascading failures and amplifying economic and societal impacts [7]. Moreover, emerging research on unmanned aerial systems (UAS) points to the growing relevance of drone-enabled threats, particularly in relation to surveillance, targeted disruption, and low-cost asymmetric attacks against critical assets [8].

Despite these advances, the existing body of literature remains fragmented in several important respects. First, studies often examine cyber, hybrid, and drone-related threats separately rather than as interacting components of unconventional terrorist strategies. Second, the economic implications of infrastructure disruption are frequently analysed independently of security-focused approaches, limiting the ability to assess systemic risk in an integrated manner. Third, much of the existing research either concentrates on sector-specific vulnerabilities or provides descriptive policy overviews without translating these insights into structured decision-making frameworks applicable within the European governance context.

This article addresses these gaps by integrating recent developments in the fields of hybrid threats, cyber-physical resilience, and critical infrastructure governance into a unified conceptual framework. Its contribution lies in the development of a three-tier risk-management model based on prediction, prevention, and resilience, which connects security and economic perspectives while reflecting the complexity of contemporary risk environments. Rather than offering a deterministic or fully operationalized solution, the model provides an analytically grounded structure designed to support strategic decision-making and to serve as a basis for further empirical validation and application.

Methodology and Analytical Approach

This article adopts a conceptual and theoretical research design aimed at developing an analytically grounded framework for managing unconventional terrorist threats to critical infrastructure. Conceptual research plays a critical role in advancing theory by integrating and reinterpreting existing knowledge, particularly in fields characterized by high complexity and limited empirical data [9]. Rather than presenting an empirical study, the paper seeks to synthesize existing academic and policy-oriented insights into a structured model that can support strategic decision-making under conditions of uncertainty.

The methodological approach is based on three complementary components. First, a targeted literature review is conducted to identify key trends, concepts, and research gaps in the academic discourse on critical infrastructure protection and emerging security threats. Literature reviews represent a well-established research methodology for structuring and synthesizing fragmented knowledge domains [10][11].

Second, the study employs a comparative policy-oriented analysis of selected European and international frameworks related to critical infrastructure protection. Policy analysis provides a systematic approach to evaluating governance mechanisms and institutional responses to complex societal challenges [12], particularly in the context of evolving regulatory frameworks such as the EU Directive on the resilience of critical entities [13].

Third, the article utilizes conceptual synthesis to integrate insights derived from both the literature review and policy analysis into a coherent analytical framework. This process reflects the need to address the systemic and interconnected nature of critical infrastructure, where disruptions may lead to cascading effects across sectors [14][15].

Typology of Emerging Threats

Unconventional terrorist threats are characterized by high technological dynamism and the capacity to disrupt critical infrastructure through methods that exceed the assumptions of traditional security scenarios. Cyberattacks represent the most rapidly evolving category, enabling adversaries to strike energy grids, transportation systems, or healthcare facilities without physical presence; research shows these attacks can trigger *"cascading failures"* across interdependent infrastructures and significantly reduce their operational availability [16].

Hybrid threats combine cyber, informational, economic, and physical instruments to destabilize states or regions, often employing non-state actors or state-supported proxy structures; their strength lies in ambiguous attribution and in the ability to target vulnerabilities not covered by standard security procedures [17]. Drone-enabled attacks further expand the tactical spectrum available to terrorist organizations by enabling low-cost, precise, and difficult-to-detect strikes on energy, transportation, and military assets; studies show that unmanned systems are particularly attractive due to their ability to bypass perimeter defences and carry improvised explosive devices or jamming technology [18].

Insider threats remain one of the most critical categories, as individuals with authorized access may intentionally manipulate technological processes, leak sensitive information, or assist external actors in bypassing physical and cyber barriers. Such attacks are especially dangerous because they combine technical expertise, legitimate access, and psychological factors that complicate detection [19]. Taken together, this typology of unconventional threats demonstrates that the contemporary security environment is shaped by adaptive, asymmetric, and difficult-to-predict attack vectors, which necessitate a systemic and multi-layered approach to risk management.

Economic Impacts of Infrastructure Disruption

Disruptions to critical infrastructure generate significant and often long-term economic impacts that extend far beyond direct physical damage and affect national productivity, employment, and fiscal stability. In the energy sector, attacks or failures can cause not only immediate power outages but also secondary losses across industry, services, and households. Studies show that large-scale blackouts lead to substantial declines in GDP, disruptions in supply chains, and increases in insurance premiums and regulatory costs [20].

In transportation, particularly aviation, maritime, and rail, any prolonged outage or blockage of key nodes translates into delays in freight movement, higher transaction costs, and major disturbances to just-in-time logistics. These effects spread across trade flows and global value chains, as demonstrated in cases involving both terrorist incidents and targeted cyberattacks on ports and logistics systems [21]. In the ICT domain, disruptions of networks and data centers directly affect the financial sector, e-commerce, and public administration; empirical analyses indicate that cyber incidents can result in losses amounting to billions, undermine investor confidence, and require substantial expenditures for restoration and the strengthening of security measures [22]. The OECD emphasizes that due to the high degree of interdependence between energy, transport, and ICT systems, economic impacts often multiply local incidents may evolve into system-wide shocks affecting multiple sectors simultaneously and requiring coordinated responses by the state, private sector, and international organizations [15].

The economic consequences of infrastructure disruption must therefore be understood not merely as recovery costs but as a complex combination of direct losses, indirect impacts, and long-term structural changes in the behaviour of firms, investors, and consumers.

Shortcomings of Current EU Risk Management

Current approaches to critical infrastructure risk management in the European Union display several systemic shortcomings that undermine their effectiveness in an environment shaped by rapidly evolving unconventional threats. One of the most frequently criticized issues is the fragmentation of responsibilities across member states and sectors, resulting in uneven

application of security standards and limited interoperability among key actors. The EU framework remains constrained by structural fragmentation, uneven national capacities, and persistent gaps in cross-border coordination, resulting in a system fragmented across national legislation, sector-specific regulations, and voluntary initiatives, which complicates coordinated responses to cross-border incidents [23].

Another major weakness is the dominance of reactive strategies that focus on protecting specific assets rather than understanding systemic interdependencies and cascading effects of infrastructure failures. The OECD stresses that most member states still prioritize single-risk prevention instead of building resilience across the entire ecosystem [15]. Insufficient information sharing on incidents and vulnerabilities represents another critical gap, despite mechanisms such as CSIRTs under the NIS Directive, data exchange is often constrained by legal barriers, distrust between the public and private sectors, and corporate concerns over reputational damage [24].

This is further compounded by slow adaptation to technological change, as the EU regulatory framework frequently responds to emerging threats - whether related to automation, drone systems, or artificial intelligence with substantial delays [25]. The shortcomings of current risk management practices are therefore not merely technical; they call for strategic modernization of governance, improved coordination across states and sectors, and a shift from isolated security policies to a holistic system of resilience.

Three-Tier Optimization Model

The proposed Three-Tier Optimization Model is designed to address the structural limitations of existing critical infrastructure protection approaches, which remain predominantly sector-specific and reactive. In contrast, the model introduces a dynamic and decision-oriented framework capable of managing the complexity, uncertainty, and interdependence associated with unconventional terrorist threats. It is structured around three mutually reinforcing layers: prediction, prevention, and resilience, each representing a distinct but interconnected phase of the risk-management process.

Prediction Tier

The predictive tier aims to enable the early identification and assessment of emerging threats before they materialize into operational incidents. Its primary purpose is to reduce epistemic uncertainty and improve situational awareness through the integration of heterogeneous data sources and analytical methods. This layer combines quantitative techniques, such as probabilistic risk assessment and data-driven modeling, with qualitative approaches, including scenario analysis and expert judgment.

Key tools within this tier include threat intelligence integration, early warning systems, data fusion platforms, and horizon scanning methodologies. These tools rely on inputs from cyber monitoring systems, sensor networks, intelligence agencies, and open-source information. The main actors involved are national security institutions, intelligence services, cybersecurity agencies, and specialized analytical units operating at both national and EU levels.

Expected outcomes of the predictive tier include improved threat detection capabilities, enhanced anticipatory governance, and more informed strategic decision-making. Illustrative indicators for evaluating performance in this layer may include incident detection time, frequency of risk reassessment, the number of integrated data streams, and the level of inter-agency information sharing.

Prevention Tier

The preventive tier focuses on reducing vulnerabilities and limiting the likelihood of successful attacks through a combination of technical, organizational, and regulatory measures. Its purpose is to strengthen the robustness of critical infrastructure systems by addressing both physical and cyber domains, as well as human and procedural factors. Key tools include redundancy mechanisms, access control systems, cybersecurity measures (e.g., network segmentation, intrusion detection), personnel security (including vetting and training), and compliance with regulatory standards such as those derived from EU frameworks (e.g., NIS2, CER Directive) [1][2]. Effective prevention requires coordinated action between public authorities, private infrastructure operators, and regulatory bodies.

The main actors in this tier include infrastructure operators, regulatory authorities, cybersecurity agencies, and public–private partnership platforms. Expected outcomes involve reduced system vulnerabilities, improved compliance with security standards, and increased resistance to both conventional and hybrid attack vectors. Illustrative indicators include compliance rates with regulatory requirements, system redundancy levels, frequency of security audits and training exercises, and results of penetration testing or vulnerability assessments.

Resilience Tier

The resilience tier represents the system's capacity to absorb, adapt to, and recover from disruptive events. Its purpose is to ensure continuity of essential services and to minimize both operational and economic impacts in the aftermath of an attack. This layer extends beyond technical recovery to include organizational adaptability, crisis management, and institutional learning. Key tools include business continuity planning, crisis management frameworks, recovery and restoration protocols, and cross-sector coordination mechanisms. Increasingly important are also mechanisms for post-incident evaluation and knowledge transfer, which contribute to long-term adaptive capacity.

The main actors include crisis management authorities, emergency services, infrastructure operators, and coordination bodies at national and EU levels. Expected outcomes include reduced recovery times, improved service restoration capabilities, and enhanced systemic adaptability. Illustrative indicators may include recovery time (time to restore critical functions), service restoration rates, performance in crisis exercises, and the implementation rate of lessons learned from past incidents. As emphasized in OECD frameworks, resilience should be understood as a multi-dimensional concept encompassing technical, organizational, and governance capacities [4].

Illustrative Application of the Model

To demonstrate the practical applicability of the proposed Three-Tier Optimization Model, this section presents a simplified illustrative scenario involving a hybrid cyber-physical attack targeting a regional electricity distribution node. The energy sector represents a critical component of national infrastructure due to its central role in ensuring the functioning of other sectors, including transport, healthcare, and communication systems. Its high degree of digitalization and interconnection also makes it particularly vulnerable to complex, multi-domain threats.

Scenario Description

The scenario assumes a coordinated hybrid attack combining a cyber intrusion into the supervisory control and data acquisition (SCADA) system with the use of an unmanned aerial system (UAS) to physically disrupt a key substation component. The cyber component is designed to manipulate operational data and delay detection, while the drone-based attack targets physical infrastructure, resulting in localized outages with potential cascading effects across the distribution network.

Application of the Prediction Tier

Within the predictive layer, the focus lies on early identification of anomalous activities across both cyber and physical domains. Threat intelligence systems would integrate data from network monitoring tools, intrusion detection systems, and external intelligence sources to identify unusual access patterns or indicators of compromise within the SCADA environment. Simultaneously, airspace monitoring and anomaly detection systems could identify unauthorized drone activity near critical infrastructure sites. Scenario analysis and risk modelling tools would be used to assess potential cascading impacts of a substation failure, including dependencies on other sectors.

The effectiveness of this tier would be reflected in indicators such as reduced detection time, increased accuracy of threat identification, and the ability to trigger early warning mechanisms prior to system disruption.

Application of the Prevention Tier

The preventive layer would aim to reduce the likelihood and impact of such an attack through a combination of technical and organizational measures. In the cyber domain, this would include network segmentation, multi-factor authentication, continuous monitoring, and regular vulnerability assessments of SCADA systems. In the physical domain, preventive measures would involve perimeter security, anti-drone technologies (e.g., detection and jamming systems), and restricted access protocols. Organizational measures would include staff training, incident response planning, and compliance with regulatory frameworks such as NIS2 and CER requirements [2]. Coordination between infrastructure operators, cybersecurity agencies, and law enforcement would be essential to ensure timely information sharing and joint preparedness.

The effectiveness of this tier would be evaluated through indicators such as system hardening levels, frequency of detected vulnerabilities, compliance rates, and the outcomes of penetration tests and security audits.

Application of the Resilience Tier

If the attack successfully disrupts operations, the resilience layer becomes critical in ensuring rapid recovery and continuity of essential services. This would involve the activation of business continuity plans, deployment of backup systems, and rerouting of electricity flows within the network to minimize service disruption. Crisis management structures would coordinate response efforts across multiple stakeholders, including energy providers, emergency services, and public authorities. Communication strategies would also play a key role in maintaining public trust and managing secondary impacts. Post-incident analysis would be conducted to identify vulnerabilities and improve future preparedness, thereby contributing to institutional learning.

The effectiveness of the resilience tier would be measured through indicators such as recovery time, service restoration rates, and performance in crisis response exercises.

Analytical Implications

This illustrative application demonstrates that the Three-Tier Optimization Model provides a structured framework for addressing complex, hybrid threats across multiple phases of the risk-management cycle. By integrating predictive, preventive, and resilience-oriented measures, the model supports a shift from reactive to anticipatory and adaptive governance. At the same time, the scenario highlights the importance of cross-sector coordination and the need to bridge the gap between technical security measures and strategic decision-making processes.

Implications for European and Global Security

Unconventional threats targeting critical infrastructure have profound implications for both European and global security, as they disrupt traditional understandings of defence, sovereignty, and international stability. In the European context, the growing technological interconnectedness among member states creates a situation in which an attack on a single national system can generate cross-border effects, a dynamic that fundamentally weakens individual governments' ability to control risks and necessitates deeper integration of cyber and infrastructure-security policies [26].

Disruptions of critical infrastructure, particularly in the energy, transport, and digital sectors, also erode the EU's strategic autonomy by limiting its capacity to respond to crises and increasing dependence on external suppliers or allies [27]. At the global level, the rapidly expanding capabilities of non-state actors, as well as state-sponsored groups, to conduct cyber and hybrid operations constitute a major destabilizing factor that blurs the boundaries between war and peace and complicates international attribution [28]. This dynamic contributes to the erosion of traditional deterrence, as the costs and risks associated with hybrid operations are relatively low while their geopolitical impact can be significant [29].

In the broader environment of global competition, infrastructure is increasingly understood as an instrument of political influence or coercion, whether through energy diplomacy, investment in transport corridors, or cyber intrusions targeting financial systems. These developments demonstrate that critical infrastructure disruption is not merely a security threat but also a strategic factor shaping the international order, amplifying great-power competition, and necessitating a new model of collective resilience based on information sharing, coordinated response, and the strengthening of democratic institutions.

Discussion

The proposed Three-Tier Optimization Model contributes to the ongoing debate on critical infrastructure protection by offering an alternative to traditional asset-based approaches, which have historically dominated both academic literature and policy frameworks. Conventional models typically focus on the identification and protection of specific infrastructure assets, emphasizing physical security measures and sector-specific risk assessments. While such approaches remain relevant, they are increasingly insufficient in addressing the complexity of contemporary threat environments characterized by interdependence, digitalization, and hybridization of risks [23][25]. In contrast, the model presented in this article adopts a system-oriented perspective that integrates multiple dimensions of risk and explicitly incorporates uncertainty, thereby aligning more closely with recent resilience-based paradigms [25][3].

A key advantage of the three-tier structure lies in its suitability for addressing high-uncertainty and low-frequency threats, which are typical of unconventional terrorist activities. Traditional risk management frameworks often rely on probabilistic models grounded in historical data; however, such data are frequently unavailable or unreliable in the context of emerging hybrid threats and novel attack vectors [30]. By combining predictive, preventive, and resilience-oriented elements, the model shifts the focus from precise prediction to adaptive preparedness and response. This aligns with contemporary approaches to risk governance that emphasize flexibility, learning, and anticipatory capacity in complex environments [12][5].

Another important contribution of the model is its explicit linkage between security and economic stability. Disruptions to critical infrastructure do not only represent operational or technical failures but also generate significant economic consequences, including supply chain interruptions, loss of productivity, and broader systemic shocks [20]. The integration of resilience as a core component of the model reflects the need to minimize not only physical damage but also economic losses and recovery time. This perspective is consistent with recent OECD and EU policy frameworks, which increasingly frame infrastructure resilience as a prerequisite for economic security and societal stability [3] European Parliament and Council, 2022a).

Furthermore, the model offers a potential contribution to addressing the persistent fragmentation of critical infrastructure governance within the European Union. Despite significant regulatory progress, including the adoption of the CER Directive and the NIS2 Directive, governance structures remain characterized by sectoral divisions, varying national approaches, and challenges in cross-border coordination [1][2]. By structuring risk management into interconnected layers that inherently require information sharing, coordination, and integration of multiple stakeholders, the proposed framework supports a more coherent and system-level approach to governance. This is in line with recent EU–NATO recommendations emphasizing the need for enhanced coordination across sectors and institutions to address systemic risks [4].

At the same time, several limitations of the model must be acknowledged. First, the framework does not provide a fully operationalized method for quantifying risks, particularly in data-sparse environments where probabilistic estimation is inherently uncertain. As such, it relies on a combination of qualitative and semi-quantitative approaches, which may introduce subjectivity into decision-making processes. Second, the model remains at a conceptual level and does not account for sector-specific differences in sufficient detail, which may limit its direct applicability without further adaptation. Third, while the model emphasizes integration across governance levels, it does not fully resolve institutional constraints such as legal fragmentation, resource disparities, or political divergences among EU member states [31].

Finally, the model does not yet incorporate advanced quantitative tools such as real-time data analytics, machine learning-based threat prediction, or dynamic system modelling, which could enhance its predictive capabilities in future applications. These limitations suggest that the proposed framework should be understood as a foundational structure for further devel-

opment rather than a fully comprehensive solution. Future research should therefore focus on the empirical validation of the model, its adaptation to specific sectors, and the integration of advanced analytical tools to improve its practical applicability.

Limitations and Future Research

This article adopts a conceptual and theoretical approach to the problem of managing unconventional terrorist threats to critical infrastructure. While this approach enables the integration of diverse strands of literature and policy frameworks into a coherent analytical model, it also entails several limitations that should be explicitly acknowledged.

First, the proposed Three-Tier Optimization Model is not empirically validated within the scope of this study. The framework is developed through conceptual synthesis and policy-oriented analysis rather than through quantitative modelling, case study comparison, or statistical testing. As a result, its practical effectiveness and predictive capacity remain to be verified in real-world settings.

Second, the analysis does not provide a detailed comparative assessment of individual European Union member states. Although the model is designed to be applicable within the broader EU governance context, it does not account for national-level differences in institutional capacity, regulatory implementation, or sectoral structure, which may significantly influence its applicability and performance.

Third, the model does not incorporate sector-specific analytical depth. Critical infrastructure sectors such as energy, transport, healthcare, and digital networks exhibit distinct risk profiles, technological characteristics, and governance arrangements. The generalized nature of the proposed framework therefore requires further adaptation before it can be operationalized in specific sectoral contexts.

Fourth, the article does not employ advanced quantitative or computational methods, such as probabilistic simulation, system dynamics modelling, or machine learning-based risk prediction. While this is consistent with the conceptual orientation of the study, it limits the model's ability to generate precise risk estimates or to support real-time decision-making processes.

These limitations open several avenues for future research. Subsequent studies could focus on the empirical validation of the model through sector-specific case studies, particularly in high-risk domains such as energy systems or digital infrastructure. Comparative analyses across selected EU member states could further refine the model by identifying institutional and regulatory variables that influence its effectiveness.

In addition, the model could be operationalized through expert-based methodologies, such as Delphi studies or structured interviews with practitioners in the fields of security, infrastructure management, and public policy. Scenario-based approaches and simulation techniques

may also provide valuable tools for testing the model under different threat conditions and for evaluating its performance in complex, high-uncertainty environments.

Finally, future research should explore the integration of advanced analytical tools, including data-driven risk assessment, artificial intelligence, and real-time monitoring systems, to enhance the predictive and adaptive capabilities of the framework. Such developments would contribute to bridging the gap between conceptual modelling and practical implementation in the field of critical infrastructure protection.

Conclusion

The growing complexity of unconventional terrorist threats targeting critical infrastructure necessitates a fundamental shift in how risk management is conceptualized and implemented. As demonstrated in this article, traditional asset-based and reactive approaches are increasingly insufficient in addressing multi-domain, interdependent, and high-uncertainty threat environments. Instead, there is a need for integrated frameworks that combine anticipatory, preventive, and adaptive capacities within a unified analytical structure.

The proposed Three-Tier Optimization Model contributes to this shift by offering a conceptual framework that links prediction, prevention, and resilience into a coherent risk-management approach. By emphasizing the integration of security and economic perspectives, the model reflects the systemic nature of critical infrastructure and its central role in maintaining societal stability. It highlights the importance of moving beyond sectoral fragmentation toward coordinated, cross-sectoral governance mechanisms, in line with recent European policy developments such as the CER and NIS2 directives [1][2].

The findings suggest that strengthening predictive capabilities can improve early threat detection and support decision-making under conditions of uncertainty, while enhanced preventive measures can reduce system vulnerabilities across both cyber and physical domains. At the same time, the resilience layer plays a crucial role in ensuring continuity of essential services and minimizing economic and societal disruptions when preventive measures fail. Together, these three dimensions form a mutually reinforcing structure that enables a transition from reactive security practices toward adaptive and forward-looking risk governance.

At a broader level, the model underscores the need to align critical infrastructure protection with economic security and systemic resilience. Disruptions to infrastructure increasingly produce cascading effects across sectors and borders, amplifying their impact on supply chains, public services, and overall economic stability. As such, effective risk management must be understood not only as a security imperative but also as a core component of sustainable economic governance [3].

At the same time, the article acknowledges that the proposed framework remains conceptual and requires further empirical validation and sector-specific adaptation. Its primary

contribution lies in structuring the problem and providing a foundation for future research and practical application rather than delivering a fully operationalized solution.

In conclusion, addressing the evolving landscape of unconventional terrorist threats requires the development of flexible, integrated, and multi-layered risk-management approaches capable of operating under conditions of uncertainty and systemic interdependence. The Three-Tier Optimization Model offers one such approach, contributing to the advancement of both academic debate and policy-oriented practice in the field of critical infrastructure protection.

About the author

PhDr. Ing. et Mgr. Ondrej Voznak, MSc. is a doctoral researcher at the Faculty of Social Studies, Masaryk University, and the Faculty of Arts, University of Hradec Králové. His academic and research interests focus on international security, hybrid threats, critical infrastructure protection, strategic autonomy, and security policy. His research combines academic insights with extensive professional experience in the military and security sectors.

References

[1] EUROPEAN PARLIAMENT a COUNCIL OF THE EUROPEAN UNION. Directive (EU) 2022/2557 on the resilience of critical entities. *Official Journal of the European Union*. 2022. Dostupné z: https://eur-lex.europa.eu

[2] EUROPEAN PARLIAMENT a COUNCIL OF THE EUROPEAN UNION. Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2 Directive). *Official Journal of the European Union*. 2022. Dostupné z: https://eur-lex.europa.eu

[3] OECD. *Government at a Glance 2025: Ensuring the Resilience of Critical Infrastructure*. Paris: OECD Publishing, 2025. Dostupné z: https://www.oecd.org

[4] NATO. *EU–NATO Task Force on the Resilience of Critical Infrastructure: Final Assessment Report*. Brussels: NATO, 2023. Dostupné z: https://www.nato.int

[5] EUROPEAN COMMISSION, Joint Research Centre. *Hybrid Threats: A Comprehensive Resilience Ecosystem (CORE) Model*. Luxembourg: Publications Office of the European Union, 2022.

[6] EUROPEAN UNION. *The Landscape of Hybrid Threats: A Conceptual Model*. Luxembourg: Publications Office of the European Union, 2021.

[7] LONGO, Francesco, NICOLETTI, Letizia a PADOVANO, Antonio. Cyber-physical systems and critical infrastructure resilience: Emerging challenges and future directions. *Electronics*. 2025, roč. 14, č. 8. ISSN 2079-9292.

[8] ŁUKASIEWICZ, Kamil a SZLACHTER, Karol. Legal and technical methods of protecting critical infrastructure against unmanned aerial vehicle threats. *Terroryzm – Studia, Analizy, Prewencja*. 2025.

[9] JAAKKOLA, Elina. Designing conceptual articles: four approaches. *AMS Review*. 2020, roč. 10,

č. 1–2, s. 18–26. ISSN 1869-814X.

[10] SNYDER, Hannah. Literature review as a research methodology: An overview and guidelines. *Journal of Business Research*. 2019, roč. 104, s. 333–339. ISSN 0148-2963.

[11] TRANFIELD, David, DENYER, David a SMART, Palminder. Towards a methodology for developing evidence-informed management knowledge by means of systematic review. *British Journal of Management*. 2003, roč. 14, č. 3, s. 207–222. ISSN 1045-3172.

[12] HOWLETT, Michael, RAMESH, M. a PERL, Anthony. *Studying Public Policy: Principles and Processes*. 4. vyd. Oxford: Oxford University Press, 2020. ISBN 978-0-19-903614-3.

[13] OECD. *Enhancing the Resilience of Critical Infrastructure Systems*. Paris: OECD Publishing, 2019. ISBN 978-92-64-98728-5.

[14] PESCAROLI, Gianluca a ALEXANDER, David. Critical infrastructure, panarchies and cascading disasters. *Natural Hazards*. 2018, roč. 92, č. 1, s. 3–15. ISSN 0921-030X.

[15] LINKOV, Igor, TRUMP, Benjamin D., POIRIER, Patrick a kol. Resilience of critical infrastructure systems: A review of recent advances and future directions. *Environment Systems and Decisions*. 2022, roč. 42, č. 4, s. 489–504. ISSN 2194-5411.

[16] DUNN CAVELTY, Myriam. 2018. *Cybersecurity Politics: Beyond the Military Metaphor*. Abingdon: Routledge.

[17] RENZ, Bettina. 2016. Russia and "Hybrid Warfare". *Contemporary Politics*, 22(3), 283–300.

[18] GETTINGER, Dan. 2019. *The Drone Databook*. New York: Center for the Study of the Drone at Bard College.

[19] SHAW, Eric a Laura Sellers STOCK. 2011. Behavioral Risk Indicators of Malicious Insider Theft of Intellectual Property: Misreading the Writing on the Wall. Symantec Research Report.

[20] ROSE, Adam a Shu-Yun LIAO. 2005. Modeling Regional Economic Resilience to Disasters: A Computable General Equilibrium Analysis of Water Service Disruptions. *Journal of Regional Science*, 45(1), 75–112.

[21] GÖSSLING, Stefan, Jonas HUMPE a Daniel SCOTT. 2013. The Global Scale, Distribution and Growth of Aviation: Implications for Climate Change. *Global Environmental Change*, 23(1), 86–94.

[22] ANDERSON, Ross, Chris BARTON, Rainer BÖHM, Richard CLAYTON, Michel J. G. van EETEN, Michael LEVI, Tyler MOORE a Stefan SAVAGE. 2013. Measuring the Cost of Cybercrime. In: BÖHME, Rainer (ed.). *The Economics of Information Security and Privacy*. Berlin: Springer, s. 265–300.

[23] MONTERO, José, Stephen H. O'REILLY a Ana V. GARCÍA. 2018. Critical Infrastructure Protection in the European Union: Progress and Challenges. *European Journal of Risk Regulation*, 9(4), 772–792.

[24] CARRAPICO, Helena a André BARRINHA. 2017. The EU as a Coherent (Cyber)Security Actor? *Journal of Common Market Studies*, 55(6), 1254–1272.

[25] ZWILLING, Marco, Anna KÖNIG a Marc KOWALEWSKI. 2022. Digital Transformation and Critical Infrastructure Protection: Challenges for European Governance. *Government Information Quarterly*, 39(3), 101–126.

[26] BENSAHEL, Nora. 2018. The Future of European Security: A Critical Infrastructure Perspective. *Survival*, 60(4), 77–98.

[27] FIOTT, Daniel. 2021. *EU Strategic Autonomy: Operationalising a Complex Concept*. Paris: EU Institute for Security Studies.

[28] LINDSAY, Jon R. 2013. Stuxnet and the Limits of Cyber Warfare. *Security Studies*, 22(3), 365–404.

[29] NYE, Joseph S. 2017. Deterrence and Dissuasion in Cyberspace. *International Security*, 41(3), 44–71.

[30] AVEN, Terje. 2015. *Risk Analysis*. 2. vyd. Chichester: Wiley.

[31] BOIN, Arjen a Martin LODGE. 2016. Designing Resilient Institutions for Transboundary Crisis Management: A Time for Public Administration. *Public Administration*, 94(2), 289–298.