ISSN 2669-2023 (print) / ISSN 2538-8959 (on-line) / **https://doi.org/10.47459/cndcgs.2026.34**

Development of Security Threats to the Czech Republic Since 2015

Jiří KALENDA[1], Marie HUDCOVÁ[1]*, Jiří BARTA[1]

[1]Crisis Management Group, Department of Military Science Theory, Faculty of Military Leadership, University of Defence, Address: Kounicova 156/65, 662 10 Brno, Czech Republic

*Correspondence: * marie.hudcova@unob.cz*

Abstract

This article addresses the reassessment of security threats to the Czech Republic in light of developments in the security environment since 2015. The aim is to update the evaluation of selected types of threats and to reflect their current characteristics, with particular emphasis on their interdependencies and their capacity to generate cascading effects. To achieve this objective, a semi-quantitative risk assessment model is applied and extended by incorporating a cascading effect coefficient. The results of the risk assessment indicate that cyberattacks, pandemics, floods, and hazardous substance releases constitute unacceptable risks, whereas the remaining assessed threats fall within the category of conditionally acceptable risks. The proposed methodological extension enables a more accurate assessment of interconnected threats. The findings may be applied in risk assessment processes within crisis management.

KEY WORDS: *Threat Analysis for the Czech Republic; security; threats; risk assessment, hazard, risk, analysis, cascading effects*

Citation: Kalenda, J.; Hudcová, M.; Barta, J. Development of Security Threats to the Czech Republic Since 2015. In Proceedings of the Challenges to National Defence in Contemporary Geopolitical Situation, Brno, Czech Republic, 7-10 September 2026. ISSN 2538-8959. https://doi.org/10.47459/cndcgs.2026.34

1. Introduction

Security represents one of the fundamental prerequisites for the stability of modern society. It cannot be reduced merely to the absence of war, armed conflict, or direct physical violence; rather, in a broader sense, it constitutes a condition for maintaining public order, protecting the life, health, and property of the population, ensuring the continuity of institutions, the functioning of the economy, and the trust of citizens in the state and its ability to fulfil its core functions, including meeting international security commitments and other defined interests [1], [2]. At present, security is understood as a multidimensional category encompassing not only the military dimension but also political, economic, social, environmental, informational, and cyber dimensions. The interconnection of these dimensions fundamentally affects the stability and resilience of both the state and society. Security must therefore be perceived as an essential framework for sustainable development, the exercise of public authority, the protection of fundamental rights and freedoms, and the preservation of the democratic constitutional order [1].

From this perspective, the *Threat Analysis for the Czech Republic* [3], approved by the Government of the Czech Republic in 2016, represented a significant step toward the systematic conceptualization of security risks at the national level. During its preparation, a wide spectrum of hazards was identified, of which 22 were classified as presenting an unacceptable level of risk. These 22 threats required priority attention across all levels of public administration [3]. The analysis established a framework for the structured assessment of serious threats, not only in terms of their probability and impacts but also with regard to the preparedness of public administration, crisis management, and civil protection. Its significance also lies in its capacity to track changes in the nature of security threats, their intensity, and their potential to disrupt the fundamental functions of the state [3].

Since 2016, however, there has been a fundamental transformation of the security environment of the Czech Republic, as well as Europe and its surrounding regions. The *Security Strategy of the Czech Republic 2023* [4] states that the security environment has further deteriorated and that Russia's war against Ukraine has definitively ended the period of peace, stability, and cooperation. This conclusion is further supported by the *Defence Strategy of the Czech Republic 2023* [8], which asserts that the likelihood of a military attack against the Czech Republic or another NATO member state is the

Peer-review under responsibility of General Jonas Žemaitis Miltitary Academy of Lithuania and University of Defence, Czech Republic.

highest since the end of the Cold War. It identifies Russia as the most serious long-term threat to the security of the Czech Republic. Alongside conventional military threats, there has been an acceleration of hybrid activities, information operations, economic coercion, sabotage, intelligence operations, and cyberattacks, all of which deliberately test the resilience of democratic states, their institutions, and critical infrastructure [4], [5]. This transformation of the security environment is not limited to the international political and military spheres but increasingly affects the internal security of the state.

The aim of this article is to reassess the relevance of the identified threats and to propose an updated evaluation reflecting the current security environment. To achieve this objective, a semi-quantitative risk assessment model is employed, extended by a coefficient capturing cascading effects of impacts. The contribution of the article lies in the methodological refinement of the assessment of complex and interrelated threats and its application to selected types of security risks. The study is based on experiences from significant crisis situations that have occurred in the Czech Republic since 2015, particularly the COVID-19 pandemic, extreme wind events, floods, and large-scale migration. It also draws on the analysis of strategic and regulatory documents of the European Union, including developments in cybersecurity policy, particularly the implementation of Directive (EU) 2022/2555 (NIS 2) [6] as well as national strategic documents and annual reports of the National Cyber and Information Security Agency, and ČSN ISO 31000 [**Error! Reference source not found.**].

2. Theoretical and Strategic Framework

Based on developments in the security environment during the previous decade, the European Parliament and the Council adopted Decision No. 1313/2013/EU on the Union Civil Protection Mechanism in 2013 [2] One of the obligations arising from this decision required EU Member States to prepare national or sub-national risk assessments (threat analyses) by December 2015. In the Czech Republic, this obligation was implemented as a task assigned to the Fire Rescue Service of the Czech Republic within the *Concept of Population Protection until 2020 with an outlook to 2030* [9], approved by the Government of the Czech Republic at the end of 2013.

The *Threat Analysis for the Czech Republic* [3] was prepared by experts from the Fire Rescue Service in 2015 and approved by the Government Resolution No. 369 on 27 April 2016. This fulfilled the obligation stemming from Decision [2] toward EU institutions. A subsequent requirement involves the regular submission, at three-year intervals, of reports on current threats based on the methodology defined in the *Threat Analysis for the Czech Republic* [3]. This task is carried out by the General Directorate of the Fire Rescue Service. The output of these regular reports contributes to the European Commission's report *Overview of Natural and Man-Made Disaster Risks the European Union May Face* [10], which monitors trends in evolving threats, with emphasis on climate change, urbanization, health risks, technological development, environmental degradation, and, above all, changes in the security environment. The report supports cross-border cooperation, prevention, and crisis management in line with the EU's objectives for disaster resilience by 2030 [11].

Given the current development of the security situation, where threats increasingly shift from hypothetical scenarios to real, ongoing, and often difficult-to-detect processes, updating the *Threat Analysis for the Czech Republic* [3] has become critically important. As these threats may undermine social cohesion, trust in public institutions, and the state's ability to prevent and effectively respond to crises, the need for updating the analysis is evident. This is not merely a revision of an older document but a necessary adaptation of the analytical and decision-making framework to new security conditions characterized by the interconnection of military, hybrid, cyber, economic, and societal sources of risk. For this reason, revising national analytical documents in the field of security is not an administrative formality but a prerequisite for the responsible execution of state security policy.

The urgency of this need is further confirmed by the fact that, in December 2023, the National Security Council was informed [12] about the update of the *Threat Analysis for the Czech Republic* [3] and the process of its further revision. In the context of the growing importance of critical infrastructure entities and the introduction of the concept of essential services, there has been a reassessment of their protection and an increased emphasis on resilience. Attention is shifting from protecting individual facilities to ensuring the functioning of essential service providers as a whole [13], [14]. The Security Information Service, in its public annual report for 2024 [15] stated that the year 2024 was among the most challenging in terms of security in the modern history of the Czech Republic. It highlighted ongoing direct and indirect activities of Russian intelligence services on Czech territory, attempts at sabotage, the spread of disinformation, increasing online radicalization among youth, and the growing influence operations of Russia and China [15].

In recent years, the cyber dimension has also become highly significant. The National Cyber and Information Security Agency reported in its *2024 Report on the State of Cybersecurity in the Czech Republic* [16] the highest number of cybersecurity incidents recorded to date—268 cases—with a substantial proportion consisting of DDoS attacks, alongside persistent threats from sophisticated campaigns attributed to state actors linked to the Russian Federation and the People's Republic of China. The report also warned that the use of artificial intelligence in cyberattacks is expected to increase in the coming years. Furthermore, it highlighted the growing number of attacks targeting operational technologies and industrial control systems, shifting cyber threats from the domain of data and service disruption to the potential for physical impacts on critical infrastructure and essential service delivery [16].

The update of the document must therefore be understood as a response to a transformed security reality, characterized by the increasing importance of strategic foresight, resilience, protection of critical state functions, and the capacity to identify and assess emerging threats in a timely manner. For both the academic and applied spheres, the updated *Threat Analysis for the Czech Republic* [3] thus represents not merely a descriptive overview of risks but, above all, a tool for shaping appropriate public policies, planning preventive measures, and strengthening the security and crisis preparedness

of the Czech Republic in conditions of a significantly deteriorated and structurally transformed security environment [11], [15], [16].

One of the key documents that has been revised is the *Security Strategy of the Czech Republic 2023* [4]. The updated version demonstrates a shift from a narrowly defined, predominantly military understanding of security toward a comprehensive, whole-of-society approach. The strategy explicitly emphasizes that, under current conditions, it is no longer possible to separate internal and external security, security in physical and digital spaces, or the security of the state, society, and individuals. It asserts that only a whole-of-government and whole-of-society approach can effectively address contemporary threats. This premise is also crucial for the analytical assessment of threats, as the current security environment is characterized by a high degree of dynamism, uncertainty, interdependence of risks, and the growing importance of factors that were previously considered secondary or ancillary.

3. Identification and Risk Analysis

The process began with a revision of the original threat register identified in 2015 [3]. As part of this revision, the original list of threats was supplemented with newly identified risks reflecting changes in the security environment and lessons learned from emergency events and crisis situations after 2015. Based on this review, threats were selected that were either not sufficiently emphasized as independent categories in the original register or for which a significant change in probability and impact occurred after 2015:

A **cyberattack resulting in a disruption of state security** was included as a distinct threat, reflecting the increasing digitalization of society and the growing dependence of the state on information systems. Compared to 2015, there has been a substantial increase in both the number and sophistication of incidents, as confirmed by annual reports of the National Cyber and Information Security Agency. A specific characteristic of this threat is its capacity to trigger cascading impacts across sectors, particularly in energy, healthcare, transport, and public administration [15], [16].

An **attack using an unmanned system (drone)** was incorporated as a new threat reflecting technological advancements and the widespread availability of drones. This threat is characterized by relatively low implementation costs and high operational flexibility, which increases its likelihood of occurrence [17]. Potential impacts primarily include disruption of critical infrastructure, threats to public space security, and risks to human life [17], [18].

A **terrorist attack** was included as a continuing relevant security threat with potentially severe consequences for human life and health, public order, social stability, and the functioning of critical infrastructure. Although the Czech Republic is not among countries with a high frequency of terrorist incidents, developments in the European security environment confirm that this threat cannot be excluded from assessment [19].

A **pandemic** was included and reassessed based on experience with the COVID-19 outbreak, which led to repeated declarations of a state of emergency in 2020 and 2021. Pandemics are characterized by extensive impacts on healthcare systems, the economy, and social stability. Their defining feature is their long-term nature and their ability to affect the functioning of the state across all sectors [20], [21], [22], [23].

Floods remain one of the most significant natural hazards, with their importance increasing in connection with climate change [24]. Repeated crisis situations, including the floods in 2024, confirm both their high frequency and the severity of their impacts on infrastructure, the economy, and territorial functioning [25], [26].

A **tornado** was included in the analysis based on the crisis situation in South Moravia in 2021, which led to the declaration of a state of danger. Although this phenomenon has a low probability of occurrence, its impacts can be catastrophic, particularly in terms of property damage and threats to the population [27].

A **hazardous substance release** is a threat reassessed based on crisis events such as the Bečva River poisoning in 2020 and the train accident involving hazardous materials (benzene) in Hustopeče nad Bečvou in 2025 [28]. These cases, together with the volume of hazardous substances transported within the Czech Republic, have demonstrated that technological accidents can have extensive impacts on the environment, public health, and the economy, and may require long-term remediation measures [29], [30], [31].

Large-scale migration was included in the reassessment of selected threats based on the experience of 2022, when a state of emergency was declared in the Czech Republic in response to the influx of refugees from Ukraine. This situation demonstrated that migration can significantly strain state capacities, particularly in the areas of accommodation, healthcare, and public administration. The impacts of this threat are primarily manifested in the social and institutional domains rather than as direct threats to human life [32].

4. Preliminary Hazard Analysis

The preliminary analysis was conducted using the same procedure as in the original *Threat Analysis for the Czech Republic*, applying a probability–impact matrix [3]. For each threat, a risk value R is determined. The risk was calculated using the following equation:

$$\mathbf{R = F \times N}$$

where F represents the frequency (probability) of occurrence and N represents the severity of consequences (impact of the threat) [3]. For the purposes of the preliminary analysis, the same matrix with a quantitative scale ranging from 1 to 3 was applied [3].

Table 1.
Criteria for Probability and Consequences in the Preliminary Analysis

Quantitative Value	Probability (Qualitative)	Verbal Description of Probability	Consequences (Qualitative)	Verbal Description of Consequences
1	Unlikely	There is only a theoretical possibility of occurrence.	Low	Minor local impact on human life and health, property, and the environment.
2	Likely	Occurrence is possible; sporadic incidence.	Significant	Greater impact on human life and health, property, and the environment at a regional level.
3	Very likely	Frequent occurrence.	Catastrophic	Very extensive impacts on human life and health, property, the environment, or economic and societal stability at the national level.

Based on the resulting value of the preliminary analysis, hazard types are classified into two groups [3]:

- Low-risk hazards ($R \leq 3$)
- High-risk hazards ($R \geq 4$)

In the case of a **cyberattack resulting in a disruption of state security**, both the probability of occurrence and the severity of impacts were preliminarily assessed as high ($F = 3$; $N = 3$), corresponding to a resulting risk value of $R = 9$. This value falls within the high-risk category and justifies the inclusion of this threat in the detailed analysis. For an **attack using an unmanned system (drone)**, both probability and severity were assessed at level two ($F = 2$; $N = 2$), corresponding to a risk value of $R = 4$. This threat is also classified as high risk and is therefore subject to detailed assessment. A **terrorist attack** was evaluated in a similar manner, with values of $F = 2$and $N = 2$, resulting in a risk value of $R = 4$. This likewise represents a high-risk category requiring further analysis. For the other threats mentioned above, a preliminary hazard analysis was not conducted, as these hazards had already been classified as unacceptable risks in the 2015 *Threat Analysis for the Czech Republic*. Nevertheless, these threats were included in the detailed multi-criteria analysis, as it is necessary to update their risk levels in light of experiences from crisis situations that have occurred since 2015.

5. Detailed Multicriteria Analysis

The multi-criteria analysis is applied to all hazards classified as high-risk in the preliminary assessment, as well as to the additional threats identified above. Its purpose is to refine the estimation of overall risk levels [3].

Risk is calculated using the following relationship:

$$\mathbf{R = F \times N,}$$

where F is expressed across ten probability intervals, as defined in Table 2 [1].

Table 2.
Frequency coefficient of potential hazard activation

Frequency of Hazard Activation (Time Interval)	Value of F
Once every few months (approx. 1–6 months or more frequently)	10
Once every several months to one year (approx. 7–12 months)	9
Once every few years (approx. 2–4 years)	8
Once every several years (approx. 5–10 years)	7
Once every few decades (approx. 2–3 decades ≈ one generation)	6
Once every several decades (approx. 4–9 decades ≈ 2–3 generations)	5
Once approximately every 100 years	4
Once every few centuries (approx. 2–4 centuries)	3
Once every several centuries	2
Once every 1,000 years or more	1

Within the multi-criteria analysis, the so-called worst-case scenario for each type of hazard is consistently considered. A scoring method (on a scale ranging from 1 to 10 points) is used to quantify information across individual criteria. In the detailed multi-criteria analysis, consequences are treated as an aggregated variable, expressed using the following relationship:

$$\mathbf{N} = (\mathbf{K_O} \times \mathbf{VK_O}) + (\mathbf{K_{ENV}} \times \mathbf{VK_{ENV}}) + (\mathbf{K_E} \times \mathbf{VK_E}) + (\mathbf{K_S} \times \mathbf{VK_S}) + (\mathbf{K_K} \times \mathbf{VK_K})$$

where $\mathbf{K_O}$ denotes the coefficient of impacts on human life and health; $\mathbf{K_{ENV}}$ represents the coefficient of environmental impacts; $\mathbf{K_E}$ denotes the coefficient of economic impacts; and $\mathbf{K_S}$ represents the coefficient of social impacts [3].

$\mathbf{K_K}$ denotes the coefficient of cascading effects, which has been incorporated into the multi-criteria analysis to reflect the interdependencies among threats. The cascading effect coefficient constitutes a methodological extension of the original model, capturing the high degree of interconnectedness of contemporary threats (see Table 3). It expresses the ability of a given threat to trigger secondary and subsequent crisis situations in other sectors, thereby amplifying the overall impact on the functioning of the state.

With the exception of the cascading effect coefficient, all other coefficient scales remain consistent with those used in the *Threat Analysis for the Czech Republic* [3].

Table 3.
Coefficient of cascading effect (VK_K)

Description of Cascading Effect	The value
No cascading effect	1
Results in one additional threat of the same type	2
Results in two additional threats of the same type	3
Results in three additional threats of the same type	4
Results in four additional threats of the same type	5
Results in three additional threats of different types	6
Results in four additional threats of different types	7
Results in two additional threats of the same type and additional threats of other types	8
Results in three additional threats of the same type and additional threats of other types	9
Results in four additional threats of the same type and additional threats of other types	10

The values of individual coefficients are determined through expert judgment by selecting from a scale ranging from 0 to 10, where a value of 0 represents a non-existent or negligible impact on the given protected interest [3]. The coefficient values were established through expert assessment by the authors of the article, who specialize in crisis management. Each author conducted the evaluation independently; subsequently, differences in the assessments were discussed, and the final values were determined by consensus.

Table 4.
Original weighting factors for determining the consequences

Protected Interest	Weighting Coefficient
Human life and health	VK_O 0.4
Environment	VK_{ENV} 0.2
Economy (property)	VK_E 0.2
Social stability	VK_S 0.2

The dominant protected interest is human life and health. To reflect the differing importance of individual domains of protected interests represented by the impact coefficients, weighting coefficients are introduced into the calculation. These weighting coefficients are determined using the Fuller method [34] Their original resulting values are presented in Table 4 [3].

Table 5.
Updated weighting factors for determining the consequences

Protected Interest	Weighting Coefficient
Human life and health	VK_O 0.34
Environment	VK_{ENV} 0.20
Economy (property)	VK_E 0.13
Social stability	VK_S 0.13
Cascading effect	VK_K 0.20

To incorporate the cascading effect coefficient into the calculation of consequences, it was necessary to reassess the weights of all evaluated protected interests. The weighting coefficients were determined using the Fuller method, based on pairwise comparison of five criteria by three expert evaluators, namely the authors of this article [34]. The resulting weighting coefficients are presented in Table 5. In their determination, particular emphasis was placed on the severity of impacts on individual protected interests of the Czech Republic and their significance for the functioning of the state and society.

The highest weight was assigned to impacts on human life and health (0.34), which represent the primary protected interest. The weight assigned to environmental impacts (0.20) reflects the fact that environmental damage often has a long-term character. The cascading effect coefficient (0.20) was assigned a comparable weight, as contemporary security threats are characterized by a high degree of interdependence and the capacity to trigger secondary and tertiary impacts across sectors. Lower weights assigned to economic impacts (0.13) and social stability (0.13) reflect the fact that these impacts are largely derived from primary impacts on life, health, and the environment.

According to the *Threat Analysis for the Czech Republic* [3] the resulting risk values derived from the semi-quantitative assessment are classified within defined intervals into three categories: **acceptable risks** (risk level 0–10), **conditionally acceptable risks** (risk level 11–29), and **unacceptable risks** (risk level 30 and above).

6. Threat Assessment Results

The determination of individual coefficient values was based on the methodology of the *Threat Analysis for the Czech Republic* [3]. This article reflects declared states of emergency in the Czech Republic since 2015, as well as threats identified by the authors through an analysis of selected security documents from the Czech Republic, as well as from Slovakia and Poland [33], [34], [35].

Cyberattack Resulting in Disruption of State Security

The cyberattack scenario was assessed using the following values: $K_O = 5$, $K_{ENV} = 1$, $K_E = 7$, $K_S = 8$, $K_K = 9$ and $F = 9$. The frequency value was determined with regard to the persistently high number of cybersecurity incidents and the increasing likelihood of attacks targeting major information systems, critical information infrastructure, and essential state services. The National Cyber and Information Security Agency reported 268 cybersecurity incidents in 2024 [16] and highlighted the growing significance of attacks targeting operational technologies and industrial control systems. At the same time, the *Security Strategy of the Czech Republic 2023* [4] states that a large-scale cyberattack may have serious consequences for the functioning and security of the state. The value $K_O = 5$ reflects the fact that cyberattacks typically do not cause direct loss of life as a primary effect; however, when targeting sectors such as healthcare, energy, or transport, they may indirectly endanger public health and safety. The value $K_{ENV} = 1$ was selected because environmental impacts of cyberattacks are generally indirect. The economic impact was expressed as $K_E = 7$, considering potential disruptions to essential services, production, logistics, and financial systems. The social impact $K_S = 8$ reflects the capacity of this threat to disrupt public administration and undermine trust in institutions. The highest partial value, $K_K = 9$ was assigned due to the exceptional potential of cyberattacks to generate cascading effects across sectors, such as disruptions in energy supply, healthcare provision, public administration, or even the triggering of secondary crisis events (e.g., special floods scenarios). The resulting consequence value is $N = 5.7$, and the overall risk value is $R = 51.3$, corresponding to the category of unacceptable risk [15], [16].

Attack Using an Unmanned System (Drone)

For the threat of an attack using an unmanned system, the following values were assigned: $K_O = 6$, $K_{ENV} = 2$, $K_E = 5$, $K_S = 7$, $K_K = 4$ and $F = 4$. The frequency value was set at four, as this type of threat does not occur regularly within the territory of the Czech Republic. However, its presence in the European security environment increases the likelihood that a similar scenario could also manifest in the Czech Republic [12]. The *Security Strategy of the Czech Republic 2023* explicitly identifies unmanned systems as a security risk, noting their potential use for direct attacks on state territory or for sabotage activities [4] The value $K_O = 6$ reflects the possibility of direct harm to individuals, particularly in the case of attacks targeting public spaces or elements of critical infrastructure. The value $K_{ENV} = 2$ corresponds to a relatively limited environmental impact, likely to occur only secondarily depending on the nature of the affected object. The economic impact $K_E =$ captures the potential material damage that unmanned systems may cause. The social impact $K_S = 7$ reflects both the security implications and, in particular, the psychological effect of such an attack in public spaces. The value $K_K = 4$ indicates that attacks on key assets may generate secondary effects in sectors such as energy, transport, or communication systems. The resulting consequence value is $N = 4.8$, and the overall risk value is $R = 19.2$, corresponding to a conditionally acceptable risk [17], [18].

Terrorist Attack

The terrorist attack scenario was assessed using the following values: $K_O = 8$, $K_{ENV} = 6$, $K_E = 6$, $K_S = 8$, $K_K = 5$ and $F = 3$. The frequency value was set at a lower level, as terrorist attacks do not occur frequently within the Czech Republic. Nevertheless, the *Security Strategy of the Czech Republic 2023* [4] identifies terrorism as a continuing relevant threat, and in 2025 the Ministry of the Interior revised the national system of terrorism threat levels. The high value $K_O = 8$ reflects the potential for direct loss of life and injury to individuals during a terrorist attack. The value $K_{ENV} = 6$ indicates that the environment may constitute a primary target of such an attack. The economic impact $K_E = 6$ captures the potential for significant material and operational damage, for example in the event of disruption to critical infrastructure such as water management systems. The social impact $K_S = 8$ reflects the strong psychological effects and the destabilizing potential of terrorism on society and the state. The value $K_K = 5$ represents the capacity of a terrorist attack to trigger secondary crisis situations, such as disruption of water infrastructure, impairment of critical infrastructure functionality, or interruptions in

the supply of water, gas, energy, or heat. The resulting consequence value is N = 6.74, and the overall risk value is R = 20.22, corresponding to a conditionally acceptable risk [19].

Pandemic

The pandemic scenario was assessed using the following values: $K_O = 9$, $K_{ENV} = 1$, $K_E = 8$, $K_S = 9$, $K_K = 9$ and F = 7. The frequency value was set at a higher level based on direct experience with the COVID-19 pandemic, which led to repeated declarations of a state of emergency across the entire territory of the Czech Republic in 2020 and 2021. In March 2020, the government-imposed restrictions on the free movement of persons, with defined exceptions, as part of crisis management measures, and the state of emergency was declared again in 2021. The pandemic thus demonstrated the capacity to trigger prolonged, large-scale, and recurrent crisis management at the national level [22], [23]. The value $K_O = 9$ reflects the direct and extensive impact on human life and health. The value $K_{ENV} = 1$ was assigned as lower, as environmental impact is not the primary consequence of this threat. The economic impact $K_E = 8$ reflects significant effects on the economy, services, and the labor market. The social impact $K_S = 9$ captures the disruption to societal functioning, public administration, healthcare, education, and everyday life. The value $K_K = 9$ was selected because pandemics represent a threat capable of triggering cascading effects across key sectors, including the overburdening of healthcare systems, social services, public administration, and broader economic and social impacts. The resulting consequence value is N = 7.3, and the overall risk value is R = 51.1, corresponding to an unacceptable risk [20].

Floods

Floods were assessed using the following values: $K_O = 7$, $K_{ENV} = 7$, $K_E = 8$, $K_S = 7$, $K_K = 9$ and F = 9. The very high frequency value reflects their repeated occurrence, as well as the fact that floods in 2024 led to the declaration of a state of emergency in the Olomouc, Moravian-Silesian, and Liberec regions [25]. The value $K_O = 7$ corresponds to the fact that floods can have extensive impacts on human life and health. The value $K_{ENV} = 7$ reflects significant impacts on watercourses, affected areas, and the potential for environmental contamination. The economic impact $K_E = 8$ was assigned due to the high level of damage to property and infrastructure. The social impact $K_S = 7$ reflects the disruption of everyday life in affected areas, public services, and the functioning of entire regions. The value $K_K = 9$ expresses the considerable potential for cascading effects across sectors, including disruptions to transport, energy supply, logistics, evacuation processes, and the recovery of affected areas. The resulting consequence value is N = 7.53, and the overall risk value is R = 67.77, corresponding to the category of unacceptable risk [25], [26].

Tornado

The tornado scenario was assessed using the following values: $K_O = 7$, $K_{ENV} = 4$, $K_E = 8$, $K_S = 7$, $K_K = 6$ and F = 4. The frequency was set at a lower level, as tornadoes do not represent a frequently occurring phenomenon in the Czech Republic. The value $K_O = 7$ reflects the potential for serious loss of life and injury to the population. The value $K_{ENV} = 4$ accounts for environmental impacts, particularly damage to forests and agricultural land. The economic impact $K_E = 8$ corresponds to substantial damage to property and infrastructure, requiring extensive repairs. The social impact $K_S = 7$ reflects disruption to the functioning of local communities. The value $K_K = 6$ represents the potential for secondary impacts, particularly in the areas of transport and energy supply. The resulting consequence value is N = 6.33, and the overall risk value is R = 25.32, corresponding to a conditionally acceptable risk [27].

Hazardous Substance Release

The hazardous substance release scenario was assessed using the following values: $K_O = 7$, $K_{ENV} = 10$, $K_E = 7$, $K_S = 6$, $K_K = 3$ and F = 8. The higher frequency and severity of this threat were derived primarily from experiences with the Bečva River contamination incident in 2020 [29] and the train accident involving benzene near Hustopeče nad Bečvou in 2025 [30]. In the case of the Bečva incident, the Ministry of the Environment reported that the contamination plume affected more than a 30-kilometre stretch of the river and resulted in the death of approximately 40 tonnes of fish. The value $K_O = 7$ reflects the risk of direct harm to human life and health, including risks faced by emergency responders. The value $K_{ENV} = 10$ was assigned due to the dominant environmental impact of this threat, including potential contamination of watercourses and soil, as well as the need for long-term remediation measures. The economic impact $K_E = 7$ reflects the high costs associated with emergency response operations, potential infrastructure damage, and environmental remediation. The social impact $K_S = 6$ captures the significant effects on communities living in the affected areas. The value $K_K = 3$ represents the potential for secondary impacts, particularly related to the long-term recovery of the affected area and associated economic consequences. The resulting consequence value is N = 6.7, and the overall risk value is R = 53.6, corresponding to the category of unacceptable risk [31].

Large-Scale Migration

The large-scale migration scenario was assessed using the following values: $K_O = 2$, $K_{ENV} = 0$, $K_E = 8$, $K_S = 8$, $K_K = 2$ and F = 6. The frequency value was determined based on the experience of 2022, when a state of emergency was declared in the Czech Republic in response to a large-scale migration wave [32]. The value $K_O = 2$ was kept low, as the direct impact on the life and health of the population is not the primary concern in this case. The value $K_{ENV} = 0$ reflects the assumption that this threat does not result in significant direct environmental impacts. The economic impact $K_E = 8$ expresses the substantial financial burden on the state and public services, particularly in relation to the provision of accommodation,

the operation of regional assistance centres, and the allocation of state housing capacities. The social impact $K_S = 8$ was assigned a high value, as the primary effects of this threat are concentrated in the strain on public administration, accommodation capacities, healthcare, as well as the education and social systems. The value $K_K = 2$ was set at a low level, as large-scale migration does not typically trigger additional crisis situations. The resulting consequence value is N = 3.2, and the overall risk value is R = 19.2, corresponding to a conditionally acceptable risk [32].

Table 6.

Threat Assessment Results

Threat	K_O	K_{ENV}	K_E	K_S	K_K	F	N	R	Category
Cyberattack	5	1	7	8	9	9	5.7	51.3	unacceptable risk
Unmanned system (drone) attack	6	2	5	7	4	4	4.8	19.2	conditionally acceptable risk
Terrorist attack	8	6	6	8	5	3	6.74	20.22	conditionally acceptable risk
Pandemic	9	1	8	9	9	7	7.3	51.1	unacceptable risk
Floods	7	7	8	7	9	9	7.53	67.77	unacceptable risk
Tornado	7	4	8	7	6	4	6.33	25.32	conditionally acceptable risk
Hazardous substance release	7	10	7	6	3	8	6.7	53.6	unacceptable risk
Large-scale migration	2	0	8	8	2	6	3.2	19.2	conditionally acceptable risk

The results presented in Table 6 indicate that the highest levels of risk are associated with floods, hazardous substance releases, cyberattacks, and pandemics, all of which have been classified as unacceptable risks. These threats are characterized not only by the high severity of their impacts but also by a pronounced cascading effect that leads to disruptions across multiple sectors simultaneously.

Floods achieved the highest overall risk value, confirming their long-term significance in the context of the Czech Republic. In contrast, threats classified as conditionally acceptable risks exhibit either a lower frequency of occurrence or a more limited capacity to trigger secondary crisis situations. Overall, the findings confirm that a key feature of contemporary threats is their complex and systemic nature.

7. Conclusion

The conducted threat analysis demonstrates that the security environment of the Czech Republic has undergone significant changes since the preparation of the original *Threat Analysis for the Czech Republic* in 2015. Not only have new types of threats emerged, but, more importantly, the nature of existing threats has evolved.

The results of the threat analysis and risk assessment indicate that the most serious threats include floods, hazardous substance releases, cyberattacks, and pandemics. These threats have been classified as unacceptable risks, as they have the potential to significantly affect human life and health, the economy, the environment, social stability, and the functioning of essential state services. Among them, floods reached the highest overall risk value. The assessment further shows that cyberattacks have become one of the key security threats, primarily due to the state's increasing dependence on digital systems and their potential to disrupt critical infrastructure, critical information infrastructure, energy systems, healthcare, transport, and public administration. Pandemics were also classified as unacceptable risks, based on recent experience (particularly the COVID-19 pandemic), which demonstrated their capacity to affect all core functions of the state over an extended period, especially the economy, public administration, healthcare, and the education system. Hazardous substance releases were likewise included among unacceptable risks, given their significant environmental impacts, particularly in terms of territorial contamination and the need for extensive and financially demanding remediation measures.

The category of conditionally acceptable risks includes attacks using unmanned systems, terrorist attacks, tornadoes, and large-scale migration. Although these threats did not reach the threshold of unacceptable risk within the applied methodology, they should not be underestimated. In the case of drone attacks and terrorist attacks, there is a risk of rapid escalation into further threats, including impacts on critical infrastructure as well as broader social consequences.

A key contribution of this article lies in the extension of the semi-quantitative risk assessment model by incorporating a cascading effect coefficient. This coefficient enables a more accurate representation of a threat's ability to trigger additional risks. Such cascading effects may include disruptions to essential services, large-scale outages of electricity, gas, food, or water supply, limitations in healthcare provision, loss of public trust in state institutions, and long-term strain on public administration.

A limitation of the assessment lies in the fact that the values of individual coefficients were determined through expert judgment by the authors. Therefore, the results should not be interpreted as a definitive quantification of risks, but rather as a semi-quantitative expert assessment enabling the comparison of selected threats. The findings also indicate that the evaluation of security threats is not a one-time process but must be conducted continuously. The security environment is

evolving more rapidly than in the past, and the state must be capable of responding to these changes not only at the level of strategic documents, but also in planning, prevention, and the preparedness of integrated rescue system components, crisis management authorities, and critical infrastructure protection. The results of this study may serve as a basis for further research into security threats.

References

1. CZECH REPUBLIC. *Security Strategy of the Czech Republic 2015*. Prague: Ministry of Foreign Affairs of the Czech Republic, 2015. [viewed 2026-03-12]. Available online: https://mzv.gov.cz/public/2a/57/16/1375879_1259981_Security_Strategy_CZ_2015.pdf
2. EUROPEAN PARLIAMENT AND COUNCIL OF THE EUROPEAN UNION. Decision No 1313/2013/EU of the European Parliament and of the Council of 17 December 2013 on a Union Civil Protection Mechanism. In: *Official Journal of the European Union* [online]. 2013, L 347, pp. 924–947 [viewed 2026-03-12]. Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32013D1313
3. CZECH REPUBLIC, Ministry of the Interior of the Czech Republic. *Threat Analysis for the Czech Republic (2015)* [online]. Prague, 2015 [viewed 2026-03-10]. Available online: https://hzscr.gov.cz/soubor/analyza-hrozeb-zprava-pdf.aspx
4. CZECH REPUBLIC, Ministry of Foreign Affairs of the Czech Republic. *Security Strategy of the Czech Republic 2023*. Prague: Ministry of Foreign Affairs of the Czech Republic [online]. Prague, 2023. [viewed 2026-03-10]. Available online: https://mzv.gov.cz/file/5123495/MZV_BS_A4_brochure_WEB_ENG__1_.pdf
5. **Řehák, D., Šplíchalová, A., Janečková, H., Ryška, O., Oulehlová, A., Michalcová, L., Hromada, M., Kontogeorgos, M., Ristvej, J.** Critical Entities Resilience Strengthening Tools to Small-scale Disasters. *International Journal of Critical Infrastructure Protection*, 2025, 49(July 2025), 100766. ISSN 1874-5482. IF 5,300. doi:10.1016/j.ijcip.2025.100766
6. European Union, 2022. Directive (EU) 2022/2555 of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union and amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972 and repealing Directive (EU) 2016/1148 (NIS 2 Directive). Official Journal of the European Union.
7. ČSN ISO 31000 (010351) Risk Management — Guidelines, 2018. Prague: Czech Standardization Agency. Available online: http://csnonline.agentura-cas.cz/
8. CZECH REPUBLIC, Ministry of Defence of the Czech Republic. *Defence Strategy of the Czech Republic 2023* [online]. Prague: Ministry of Defence of the Czech Republic [online]. 2023. [viewed 2026-03-12]. Available online: https://www.mo.gov.cz/assets/en/ministry-of-defence/basic-documents/defence-strategy-of-the-czech-republic_2023_final.pdf
9. CZECH REPUBLIC, Ministry of the Interior of the Czech Republic – Directorate General of Fire and Rescue Service of the Czech Republic. *The Concept of Population Protection till 2020 with the outlook to 2030* [online]. Prague: Ministry of the Interior of the Czech Republic, 2013 [viewed 2026-03-015]. ISBN 978-80-86466-50-7. Available online: https://hzscr.gov.cz/soubor/koob-2020-2030-aj-2016-pdf.aspx
10. EUROPEAN COMMISSION. *Overview of natural and man-made disaster risks the European Union may face: 2020 edition* [online]. Luxembourg: Publications Office of the European Union, 2021 [viewed 2026-03-15]. ISBN 978-92-76-24754-8. Available online: https://civil-protection-knowledge-network.europa.eu/media/overview-natural-and-man-made-disaster-risks-european-union-may-face
11. EUROPEAN COMMISSION. Commission Recommendation (EU) 2023/215 of 8 February 2023 on *Union disaster resilience goals*. Official Journal of the European Union. 2023, vol. 66, L 31, pp. 1–11. ISSN 1977-0677. Available online: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=uriserv:OJ.C_.2023.056.01.0001.01.ENG
12. CZECH REPUBLIC. National Security Council. *Record of the NSC meeting held on 7 December 2023* [online]. 7 December 2023 [cited 2026-03-10]. Available online: https://vlada.gov.cz/cz/ppov/brs/cinnost/zaznamy-z-jednani/zaznam-ze-schuze-brs-konane-dne-7--prosince-2023-211175/
13. Zákon č. 266/2025 Sb. *Zákon o odolnosti subjektů kritické infrastruktury a o změně souvisejících zákonů (zákon o kritické infrastruktuře)*
14. **Řehák, D., Šplíchalová, A., Janečková, H., Oulehlová, A., Hromada, M., Kontogeorgos, M., Ristvej, J.** Critical Entities Resilience Assessment (CERA) to small-scale disasters. *International Journal of Disaster Risk Reduction*, 2024, 111(September 2024), 104748. ISSN 2212-4209. IF 4,500. doi:10.1016/j.ijdrr.2024.104748
15. SECURITY INFORMATION SERVICE – INTELLIGENCE SERVICE OF THE CZECH REPUBLIC. *Annual Report of the Security Information Service for 2024* [online]. Prague: Security Information Service, 2025 [cited 2026-03-22]. Available online: https://www.bis.cz/public/site/bis.cz/content/vyrocni-zpravy/2024-vz-aj.pdf.
16. NATIONAL CYBER AND INFORMATION SECURITY AGENCY. *2024 Report on the State of Cybersecurity in the Czech Republic* [online]. Brno: National Cyber and Information Security Agency, 2025 [cit. 2026-03-25]. Available online: https://nukib.gov.cz/download/publications_en/2024_Report_on_the_State_of_Cybersecurity_in_the_Czech_Republic.pdf
17. **Engelová, T.** Dokázalo by se Česko ubránit útoku dronů? U ojedinělého incidentu je obrana těžká. In: *HlídaciPes.org*[online]. 2024. [cit. 2026-04-28]. Available online: https://hlidacipes.org/dokazalo-by-se-cesko-ubranit-utoku-dronu-otazka-na-kterou-nikdo-nema-odpoved/

18. *Neoprávněné přelety dronů mohou být nebezpečné. Český AIRSEC před nimi chrání obyvatele a kritickou infrastrukturu bez zbytečné střelby* [online], 2025. In: Roklen24 [cit. 2026-04-28]. Available online: https://roklen24.cz/?quick_news=neopravnene-prelety-dronu-mohou-byt-nebezpecne-cesky-airsec-pred-nimi-chrani-obyvatele-a-kritickou-infrastrukturu-bez-zbytecne-strelby
19. *Audit národní bezpečnosti* [online], 2016. Praha: Ministerstvo vnitra ČR, odbor bezpečnostní politiky a prevence kriminality [cit. 2026-03-30]. Available online: https://www.vlada.cz/assets/media-centrum/aktualne/Audit-narodni-bezpecnosti-20161201.pdf
20. **Miklánková, L.** *Stát v pasti: dopady pandemie na postoje, důvěru a chování veřejnosti* [online]. In: Akademie Věd České republiky, 25. 06. 2025 [cit. 2026-04-28]. Available online: https://www.avcr.cz/cs/veda-a-vyzkum/socialne-ekonomicke-vedy/Stat-v-pasti-dopady-pandemie-na-postoje-duveru-a-chovani-verejnosti/
21. COVID-19: reakce EU na ekonomické důsledky pandemie, 2022. Evropská rada Rada Evropské unie [online]. [cit. 2026-04-28]. Available online: https://www.consilium.europa.eu/cs/policies/coronavirus-pandemic/covid-19-economy/
22. *Rozhodnutí vlády o zákazu volného pohybu osob* [online], 2020. Vláda České republiky [cit. 2026-04-27]. Available online: https://vlada.gov.cz/cz/media-centrum/aktualne/rozhodnuti-vlady-o-zakazu-volneho-pohybu-osob-180358/
23. Česká republika. *Usnesení vlády č. 70/2022 Sb., o vyhlášení nouzového stavu* [online]. [cit. 2026-04-20]. Available online: https://www.zakonyprolidi.cz/cs/2022-70
24. **Kincl, P., Oulehlová, A.** Assessment Criteria for Municipality Territory Resilience to Anthropogenic Threats. In: *Trends and Future Directions in Security and Emergency Management*. Cham: Springer, 2022, s. 209-224. ISBN 978-3-030-88907-4. doi:10.1007/978-3-030-88907-4_11
25. POVODNĚ 2024 VYHODNOCENÍ REAKCE NA KRIZOVOU SITUACI, 2025. *MINISTERSTVO VNITRA ČESKÉ REPUBLIKY* [online]. 15 [cit. 2026-04-27]. Available online: https://mv.gov.cz/soubor/povodne-2024-vyhodnoceni-reakce-na-krizovou-situaci-ukol-uks-c-29.aspx
26. **Kramář, R.** Hasičské jednotky ukončily odstraňování následků tornáda na Jižní Moravě. *Hasičský záchranný sbor České republiky* [online]. 2021. Česká asociace pojišťoven [cit. 2026-04-28]. Available online: https://hzscr.gov.cz/clanek/hasicske-jednotky-ukoncily-odstranovani-nasledku-tornada-na-jizni-morave.aspx
27. Náklady na krizové řízení po tornádu na jižní Moravě jsou 50 milionů. Šly na jídlo i likvidaci odpadů, 2021. *IRozhlas* [online]. [cit. 2026-04-28]. Available online: https://www.irozhlas.cz/zpravy-domov/tornado-na-jizni-morave-naklady-na-krizove-rizeni_2108232108_btk
28. **Polívka, L., Mika, J.O., Barta, J.** Safety of Dangerous Goods Transport by Rail in the Czech Republic. Chemické Listy, 2026, 120(3), 154–161. https://doi.org/10.54779/chl20260154.
29. *Ministr Brabec: Vedle usvědčení pachatele je klíčová obnova Bečvy po katastrofě* [online], 2020. In: Ministerstvo životního prostředí [cit. 2026-04-27]. Available online: https://mzp.gov.cz/cz/pro-media-a-verejnost/aktuality/archiv-tiskovych-zprav/ministr-brabec-vedle-usvedceni-pachatele-je
30. Ochmanová, K. *80 dní od havárie vlaku s benzenem jsou koncentrace nebezpečné látky v okolí téměř nulové* [online]. In: Hasičský záchranný sbor kraje, 16. 5. 2025 [cit. 2026-04-28]. Available online: https://hzscr.gov.cz/clanek/80-dni-od-havarie-vlaku-s-benzenem-jsou-koncentrace-nebezpecne-latky-v-okoli-temer-nulove.aspx
31. **Barta, J., Loufková, L., Mika, J.O.** Improving Safety in the Transport of Hazardous Chemicals by Road in the Czech Republic. In: 16th International Scientific Conference on Sustainable, Modern and Safe Transport. Elsevier B.V., 2026, roč. 2026, č. Volume 93, s. 1083-1095. ISSN 2352-1465. doi:10.1016/j.trpro.2025.12.046
32. BEZPEČNOSTNÍ ASPEKTY MIGRACE. *Ministerstvo vnitra České republiky* [online]. [cit. 2026-04-28]. Available online: https://mv.gov.cz/chh/clanek/bezpecnostni-aspekty-migrace.aspx
33. The statements, opinions and data contained Official Website of the Polish Government. Gov.pl [online]. [accessed 13 Feb. 2026]. Available online: https://www.gov.pl
34. **Čubranić-Dobrodolac, M.; Jovčić, S.; Bošković, S.; Babić, D.** A Decision-Making Model for Professional Drivers Selection: A Hybridized Fuzzy–AROMAN–Fuller Approach. *Mathematics* 2023, *11*, 2831. Available online: https://doi.org/10.3390/math11132831
35. **Coronicova Hurajova, J.; Hajduova, Z.** Multiple-Criteria Decision Analysis Using TOPSIS and WSA Method for Quality of Life: The Case of Slovakia Regions. Mathematics 2021, 9, 2440. https://doi.org/10.3390/math9192440 Available online: https://www.mdpi.com/2227-7390/9/19/2440