# The Current State of Effectiveness of the Security System of the Slovak Republic

**Katarína Miňová**

https://doi.org/10.33542/VSS2024-2-6

***Abstract***

*The objective of this article is to analyze the current state of the Slovak Republic's security system, with a particular focus on its effectiveness and the role of the Security Council of the Slovak Republic within the crisis management framework. The paper examines the legislative and organizational aspects of the security system, emphasizing its capacity to respond to contemporary challenges such as hybrid and cyber threats. Using a SWOT analysis, the study identifies strengths, weaknesses, opportunities, and threats, while comparing Slovak practices with those of other Visegrad Group countries, particularly the Czech Republic and Poland. Examples from crisis management during the COVID-19 pandemic and other emergencies illustrate the practical implications of the system's operations. Based on these findings, the article proposes recommendations for enhancing the system's coordination, digitalization, and resilience, offering a framework for more efficient crisis response at national, regional, and local levels.*

***Keywords:*** *Security system of the Slovak Republic, Security Council of the Slovak Republic, crisis management, digitalization, cyber-security, threats, opportunities, strengths, weaknesses, SWOT analysis*

## Introduction

The security system of the Slovak Republic (SR) is a complex set of institutions, legal instruments, procedures and measures that ensure the protection of the state, its citizens and strategic interests against internal and external threats. Examining this system is essential for identifying its strengths and weaknesses, which allows for the formulation of recommendations for its streamlining and adaptation to the changing security challenges that the Slovak Republic faces today and needs to be able to respond to effectively.

The security system is the key element on which the basic ability of the state to provide its essential functions and services depends. The examination of the security system of the Slovak Republic is therefore crucial not only for security policy experts, but also for policy makers, academics and the general public. The results of such research can contribute significantly to building a resilient and effective system capable of meeting current and future challenges.

The aim of examining the security system of the Slovak Republic for the purposes of this paper is to assess whether the current legislation and structures meet the needs of security in the current geopolitical and technological environment. Verifying how effectively a security system can respond to different types of threats, including hybrid attacks, cyber threats, natural disasters and pandemic crises. Analysis of good practice examples of countries with similar security challenges as the Visegrad Four (V4) countries. And on the basis of the above - a proposal for specific measures to optimise processes, increase the reliability of the system and strengthen its coordination.

## 1. Historical context

The development of the security system of the Slovak Republic is closely linked to the historical, political and security challenges faced by the new state after its establishment in 1993. Since then, the security system has undergone several stages of transformation, adapting to internal needs and international commitments.

After the division of the Czech and Slovak Federative Republic, the security system of the Slovak Republic was formed on the basis of institutions taken over from the federal structure, with an emphasis on the creation of independent security and defence mechanisms.

However, the security system as a complex mechanism is first mentioned in the Security Strategy of 2001, which stresses the need to build it, in the context of the accession to NATO and the EU, so that the state has a governing body that will ensure a unified system of management in crisis situations (Ušiak, 2021). In the conclusion of the strategy from 2001, the Government of the Slovak Republic undertook to build the Security System of the Slovak Republic, which will represent a complex, integrated, functionally and structurally purposefully arranged system, in which the competences, i.e. rights and duties, responsibilities and the mutual mechanism of relations between its elements will be specifically defined, so that this security system is capable of fulfilling its mission to plan, manage, coordinate tasks, measures and activities of its elements to guarantee the security of the state in peacetime, in crisis situations and in war, with effective use of the internal resources and means of the state and international support (Security Strategy of the Slovak Republic, 2001)

According to the Security Strategy of the Slovak Republic of 2001, the security system should be able to analyse the security environment, its global, regional and sub-regional aspects, classify security risks and threats to the Slovak Republic and the tendencies of their development, determine procedures and measures for the prevention and elimination of security risks and threats and the resolution of crisis situations in accordance with available resources and capacities, ensure effective management and coordination of forces and means in the prevention and elimination of individual types of security risks, threats and crisis situations, with a precise definition of competences and interrelationships between the National

Council of the Slovak Republic, Government of the Slovak Republic, the President of the Slovak Republic and other public authorities, legal entities and natural persons, to achieve the required degree of interoperability with the security systems of the Member States of the North Atlantic Alliance and its neighbours, enabling effective international cooperation of the entire system and its individual elements, to operate as an integral part of the mechanism of state management in accordance with the constitutional legal order of the Slovak Republic, to ensure the required level of sensitivity and flexibility, to have the necessary scientific and theoretical background and qualified personnel, to ensure its continuous readiness and operational capability. (Security Strategy of the Slovak Republic, 2001)

A significant event was the adoption of Act No. 110/2004 Coll. on the Activity of the Security Council of the Slovak Republic at the Time of Peace, which established the legal basis for its activities as a coordinating body of the Government (Act No. 110/2004 Coll.).

Slovakia's accession to NATO and the EU in 2004 brought significant changes in security policy. The Security Council of the Slovak Republic assumed the role of coordinator in the implementation of international commitments in the field of defence, security and crisis management. This integration required the alignment of national security measures with NATO and EU standards, thus increasing the strategic importance of the Council (Statute of the Security Council of the Slovak Republic, 2024).

The 2005 Security Strategy of the Slovak Republic mentions the security system as a decisive means of security policy, a multifaceted complex consisting of foreign policy, economic, defence, internal security, social, rescue and ecological instruments and their interrelations. The basic prerequisite for the management, construction and development of the security system of the Slovak Republic are effectively functioning legislative, executive and judicial bodies. They are responsible for the readiness and actionability of crisis management tools and the timely adoption and implementation of measures aimed at guaranteeing the security of citizens and the state. However, despite this, the 2005 Security Strategy, reflecting NATO and EU membership, still states in its Article 38 that the Security System of the Slovak Republic *will be* capable, i.e. it could not yet be considered ready. Thus, in the future, according to this strategy, it should be able to provide a unified management system in all crisis situations; identify the emerging crisis situation and provide early warning; analyse the impact of the crisis situation on the security interests of the Slovak Republic and propose the manner of participation of the Slovak Republic in its resolution; prevent the emergence of crisis situations and, if they arise, eliminate them at their outset; respond to the most likely threats, adapt to changes in the security situation, including responding to unexpected threats; ensure the rapid elimination of the consequences of the crisis situation and the restoration of the original situation; and guarantee the continuity of its functioning. (Security Strategy of the Slovak Republic, 2005)

After 2010, the Slovak security system faced new challenges such as hybrid threats, cyber-attacks and migration crises. Although these phenomena were already present in the international, broader regional and Slovak security environment a few years after the adoption of the 2005[3] Security Strategy, the Slovak Republic did not respond strategically and conceptually to them until 2021, when the government adopted a new Security Strategy for the Slovak Republic. In its Article 45, the Security Strategy for the Slovak Republic sets as its main priorities for the security system to ensure an effective and efficient management system in all crisis situations; to identify emerging crisis situations and provide early warning; to analyse the impact of a crisis situation on the security interests of the Slovak Republic and to propose solutions; to prevent the emergence of crisis situations and to increase the resilience of the state and society, and to suppress such situations in their initial stages if they arise; respond to confirmed threats and adapt to changes in the security situation, including reacting to unexpected threats; ensure the rapid removal of the consequences of a crisis situation and the restoration of the original state; guarantee the continuity of its functioning; improve the sharing of information between the individual elements of the security system; systematically practise and evaluate its functionality. (Security Strategy of the Slovak Republic, 2021)

Another milestone in the historical development was the adoption of the new Concept of the Security System of the Slovak Republic (2023), which reflects these challenges and redefines the role of the Security Council of the Slovak Republic. The government took this step in relation to the prioritisation of the reform of the Slovak security system in its 2020 Programme Statement, which spoke of modernising and improving the security system to respond to current security challenges, including hybrid threats and the need for strong coordination between the components of the security system (New Concept of the Security System of the Slovak Republic, 2023, Programme Statement of the Government of the Slovak Republic, 2021).

The new Concept replaced the 2002 concept materials. It is based on making the security system more efficient without setting up new institutions. The focus of increasing the resilience of the state will lie in the coordination of individual entities by the Security Council of the Slovak Republic. The Security Council of the Slovak Republic is presented in the concept as the main coordinating body responsible for effective response to crisis situations and for strengthening the resilience of the state to security threats. Historically, the Security Council of the Slovak Republic has played a key role in coordinating crisis responses, especially in the case of major crises such as floods, pandemic situations or NATO military exercises. In the new concept, its role is strengthened by introducing systematic planning of crisis responses,

[3] For example, the terrorist attacks on the US in September 2001 or the cyber attacks on Estonia in 2007.

the inclusion of an executive vice-chairman and an emphasis on a unified methodology for all components of the security system (Act No. 110/2004 Coll., New Concept of the Security System of the Slovak Republic, 2023). The concept also envisages the strengthening of the individual executive components in terms of personnel, expertise and material. The composition of the Central Crisis Management Staff should be modified - its management structures will include an executive vice-chairman in the person of the minister of the ministry responsible for the implementation of tasks according to the specific type of threat. The security system should thus be gradually transformed from the current one to ensure uniformity of decision-making and separation of decision-making, advisory and executive functions and powers of the crisis management bodies. The concept contains two models of the security system, which differ in the extent of the transformation and changes needed to the current security system. The first model proposes strengthening the role of the Security Council of the Slovak Republic in the decision-making process in dealing with a crisis situation. However, its disadvantage is the need to amend the Constitution of the Slovak Republic and the Constitutional Law on State Security during War, State of War, State of Emergency and State of Emergency with regard to the status of the Government of the Slovak Republic and the Security Council of the Slovak Republic. The second model states that the main decision-making body of the security system in any situation, including crisis situations, should be the government alone. At the same time, it proposes the integration of the Central Crisis Management Staff into the Security Council of the Slovak Republic (New Concept of the Security System of the Slovak Republic, 2023). The new government elected in 2023 emphasises stability, peace and security for citizens. The programme declaration focuses on protection from external threats and strengthening national self-confidence and sovereignty, with less emphasis on specific modernisation elements of the security system. It emphasises Slovakia's internal security and sovereignty. Although it supports the security system, the text does not explicitly mention the centralisation of crisis management or improved coordination between the components. In the area of hybrid and cyber threats, the current government focuses more on sovereignty and the protection of national interests, with less emphasis on cyber and hybrid security compared to the previous government. For the current government, the focus on internal stability is rather important and it does not specify any specific planned changes in the functioning of the security system among its priorities, while its areas of interest are more focused on social stability and internal security (Programme Statement of the Government of the Slovak Republic, 2023). It is questionable to what extent the proposals of the new Concept of the Security System, which could potentially aim at strengthening the competences of municipalities as important actors of the security system in the field of crisis management and also at improving the conditions for their mutual cooperation in managing crises and emergencies such as the pandemic crisis, will be implemented during the mandate of the current government (the electoral period 2023 - 2027), e.g. following the example of some other European countries. The current government can probably be expected to focus on maintaining Slovakia's sovereignty and internal security, but so far without a detailed plan for the modernisation and centralisation of the security system, with the exception of the draft of a new comprehensive framework of processes and procedures for crisis management in the Slovak Republic from the Ministry of the Interior in the spring of this year. (Proposal for a new comprehensive framework of processes and procedures for crisis management in the Slovak Republic, 2024; The Ministry of Interior of the Slovak Republic, 2024)

## 2. Theoretical and legal definition

At present, the Security System is defined without changes by the original legislation in force - the Constitution of the Slovak Republic, which in its Article 1 and Article 102 sets out the basic principles of protection of the sovereignty and security of the state. It is also defined by the Constitutional Act on State Security in Wartime, During Hostilities, Martial Law and State of Emergency No. 227/2002 Coll. as amended, which regulates the way of managing the state during a state of threat and war, when specific defence and protection mechanisms are activated. In times of war, the Government of the Slovak Republic assumes full responsibility for the management of the State and the Security Council of the Slovak Republic acquires exceptional coordinating powers. Furthermore, it is also Act No. 387/2002 Coll. on the Control of State in Crisis Situations Except for Wartime and During a State Hostilities, which lays down the basic principles of the functioning of the security system and its structure. It defines the roles of the government, ministries, local authorities and other entities in dealing with crisis situations (Act No. 387/2002 Coll.). Furthermore, it is Act No. 110/2004 Coll. on the Activity of the Security Council of the Slovak Republic at the Time of Peace, which defines the role of the Security Council of the Slovak Republic as the coordinating body of the Government for security policy and crisis management, and the Statute of the Security Council of the Slovak Republic, which specifies the organisational structure and mechanisms of the Security Council of the Slovak Republic (Act No. 110/2004 Coll., Statute of the Security Council of the Slovak Republic, 2004).

The Security System of the Slovak Republic in these legal sources is a complex set of legal, organisational and functional measures that ensures the protection of the state, its citizens and its interests against internal and external threats. It ensures the sovereignty of the State, the protection of territorial integrity, political stability and the security of the population. It integrates defence, security, economic, information and environmental measures into a unified system of response to crises and threats. It includes activities such as crisis management during peacetime and emergencies, defence mechanisms activated in times of state threat and war, coordination between the executive bodies of the state, municipalities and security forces.

## 3. The structure of the security system of the Slovak Republic

The top level is represented by **the executive bodies of the state**. *The President of the Slovak Republic* is the supreme representative of the State and Commander in Chief of the armed forces of the Slovak Republic (Constitution of the Slovak Republic, Article 102). He has the power to declare a state of war on the proposal of the Government. In times of war or state threat, he coordinates the cooperation of the armed forces with the Security Council of the Slovak Republic and the Government of the Slovak Republic. *The Government of the Slovak Republic* is responsible for the overall management of the security system of the Slovak Republic (Act No. 387/2002 Coll.). In peacetime, it organises the preparation of the state for crisis situations, including the development of strategic plans. In times of war or threat to the state, it has the authority to manage all components of the security system, including the armed forces and civil protection. (Šimák, 2016)

**The Security Council of the Slovak Republic** plays an important role in the security system of the Slovak Republic, which is an advisory, initiative and coordinating body of the Government of the Slovak Republic, coordinates strategic security planning and crisis management, monitors threats and proposes measures to deal with them (Act No. 110/2004 Coll., Statute of the Security Council of the Slovak Republic). Its key competences include the preparation of security policy and strategic documents; supervision of the fulfilment of Slovakia's international obligations within NATO and the EU; coordination of the activities of security system entities and their preparation for crisis management (Act No.110/2004 Coll.), activation of crisis plans in emergency situations and in a state of war. The Statute provides that the Security Council of the Slovak Republic has nine members, including the chairman (Prime Minister) and vice-chairmen. The Chairman of the Security Council of the Slovak Republic is the Prime Minister of the Slovak Republic, and the members are representatives of relevant ministries and state administration bodies. The committees for specific areas, such as defence planning or civil protection, provide expert preparation of proposals (Šimák, 2016).

At the same time, **ministries and other central government bodies, such as** the *Ministry of Defence of the Slovak Republic*, which manages the Armed Forces of the Slovak Republic and is responsible for their readiness for the defence of the state (Act No.321/2002 Coll. on the Armed Forces of the Slovak Republic), and also coordinates military operations in times of war and crisis deployment of forces in peacekeeping operations, also play an important role in the security system of the Slovak Republic. Furthermore, the *Ministry of the Interior of the Slovak Republic*, which manages crisis management in the civilian sector, including the police, fire brigades and integrated rescue system components (Act No. 387/2002

Coll.), and is responsible for the organisation of civil protection of the population and the protection of public order. Furthermore, the *Ministry of Foreign and European Affairs of the Slovak Republic*, which coordinates the international security policy of the Slovak Republic and is responsible for the fulfilment of the international obligations of the Slovak Republic within NATO, the EU and the UN. The *Ministry of Finance of the Slovak Republic* ensures the financing of the security system, establishes budgetary frameworks for crisis management and defence planning. (Šimák, 2016)

**Regional and local crisis management units**, such as *regional crisis management staffs* established at the level of municipalities, are also an important part of the security system, coordinating crisis management between municipalities and central authorities. They prepare response plans for crisis situations such as floods or pandemic threats. Furthermore, *municipal and city crisis management staffs* are also responsible for the initial response to local threats, including natural disasters and accidents. They work with police, firefighters and medical facilities to ensure the protection of the population (Šimák, 2016).

The Security System of the Slovak Republic is also composed of **supporting components** of the security system, such as *the Armed Forces of the Slovak Republic*, which represent the basic component of the defence of the state, deployed for the defence of the territory or in the framework of international operations. They provide logistical and personnel support during crises, such as floods or pandemic measures. Then there is *the Integrated Rescue System (IRS)*, which includes the police, firefighters, emergency medical services and other bodies. It ensures a coordinated response to emergencies such as traffic accidents, fires or evacuations of the population. Last but not least, the Security System of the Slovak Republic also includes the *intelligence services*, *the Slovak Information Service (SIS)* and *military intelligence*, which ensure the collection and evaluation of information on security risks. They support strategic planning and operational responses to threats. (Šimák, 2016)

## 4. Efficiency analysis of the security system of the Slovak Republic

For the purposes of this paper, the analysis is conducted through the so-called SWOT analytical technique, used to strategically assess the internal and external factors that affect the performance of an organisation, system or project. It specifies four main categories of assessment: Strengths, Weaknesses, Opportunities and Threats. It is a versatile and practical tool that not only assesses the current state, but also provides a framework for strategic decision-making and planning. It allows comparisons to be made between different actors or systems, which is useful, for example, when assessing good practice in an international setting. The analysis of the effectiveness of the Security System of the Slovak Republic is based on the currently valid legislation, concrete examples of crisis management in the Slovak Republic and these values are compared with examples of good practice from abroad (Czech Republic and Poland) and also the proposals for a new concept of the Slovak security system and the current proposal of the Ministry of Interior of the Slovak Republic regarding the creation of a new comprehensive framework of processes and procedures for crisis management in the Slovak Republic.

### 4.1 Strengths

The Security System of the Slovak Republic is characterised by a number of *strengths* that confirm its robustness. Its main strengths include *a comprehensive legislative framework*, which is firmly anchored in laws such as Act No. 387/2002 Coll. on Control of State in Crisis Situations Except for Wartime and During a State Hostilities. This framework enabled effective management during the COVID-19 pandemic, for example through the introduction of the COVID automat. (Ministry of Health of the Slovak Republic, 2021) In this area, the Slovak system can be compared with the Czech Republic, which has a similarly effective Crisis Management Act No. 240/2000 Coll. However, according to the new Security System Concept, it would be advisable to unify this robust legislative framework so that the various laws dealing with the security system are consolidated. This challenge is partly answered by the proposal for a new comprehensive framework of processes and procedures for crisis management in the Slovak Republic, which was presented by the Minister of the Interior in early 2024. As stated in the material discussed and approved by the Government, the subject of this forthcoming project is the proposal of a new comprehensive framework of processes and procedures for crisis management, its implementation into practice and the creation of a new entity subordinate to the Minister of the Interior (the Office for Crisis Management), which will be responsible for the entire life cycle of crisis management in Slovakia, i.e. not only crisis management, but also prevention, preparation and subsequent recovery. This entity will have its own resources (people, assets), supra-ministerial competences and will be the sole representative in this area both inside and outside the state (similar to the Police Corps or the Armed Forces of the Slovak Republic) (Proposal for a new comprehensive framework of processes and procedures for crisis management in the Slovak Republic, 2024; (The Ministry of Interior of the Slovak Republic, 2024).

*The involvement of regional and local governments* is another **strong element**. Based on the principle of subsidiarity, municipalities have an indispensable role to play in dealing with crisis situations.  In practice, municipalities and cities have demonstrated their ability to respond to crisis situations by setting up collection and vaccination points during a pandemic. (Košice Self-Governing Region, 2022 and 2022; Government Resolution No. 110/2021). A proposal from the current Ministry of the Interior to create an Office for Crisis Management centralizes crisis management into a new entity subordinate to the Minister of the Interior. This step eliminates inconsistency and duplication of competences. On the other hand, the currently planned project of the Office for Crisis Management, which will be centrally responsible for crisis management, raises a slight concern about the extent to which crisis management is moving towards centralisation, which ultimately may not be worthwhile in terms of capacity, personnel or organisation in the 21st century, when the trend in modern democratic states is to decentralise rather than to centralise, when it comes to managing crises in the state.

**The strengths** also include *Slovakia's involvement in international cooperation in the field of security* and the fulfilment of the obligations and rights arising therefrom. Slovakia's foreign policy orientation plays a special role in this area, as its membership in organisations such as the North Atlantic Treaty Organisation and the European Union gives it access to best practices, civil protection mechanisms and other resources. For example, Slovakia had the opportunity to use EU mechanisms to provide medical supplies during the pandemic.

### 4.2 Weaknesses

With regard to **the weaknesses** of the Security System of the Slovak Republic, it is possible to note in particular *the fragmentation of competences* between the central level of state management and local state or local government bodies. This weakness is one of the most pronounced. Departmental thinking, which causes fragmentation of competences between central authorities, regional and local entities, weakens the effectiveness of the security system as a whole.  This weakness was evident during the pandemic when there was confusion between central measures and their implementation at the local level. (Prokopčáková, 2024) For comparison, the Czech Crisis Management Act No. 240/2000 Coll. precisely defines the competences of the different levels of governance (state, regional and local). In contrast to Slovakia, the Czech Republic has a stronger involvement of regional authorities, which function as an intermediate step between the government and municipalities, which improves information transfer and uniformity of measures. Regional authorities thus have a significant role to play in the crisis management coordination, thus eliminating confusion between central and local actors. To this end, the Czech government has established an integrated information system for crisis management, which allows for efficient information sharing between central and regional authorities. Regional health stations were key in epidemiological monitoring and setting up measures. Their direct connection to the central government allowed for rapid implementation of regulations. During the pandemic, the Czech regions proved to be flexible units that could adapt measures to local needs in accordance with centrally established rules. (Act No. 240/2000 Coll., on Crisis Management; Ministry of Health of the Czech Republic, 2022; Crisis Portal, 2022)

In this context, the New Security System Concept recommends the establishment of a digital platform for coordination. The proposal of the current Minister of the Interior (2024) partly answers this call because the proposal presented for the creation of the Office of Crisis

Management centralizes crisis management in a new entity that reports directly to the Minister of the Interior. This step eliminates inconsistencies and duplication of competences. And since Slovakia has lacked a sufficiently interconnected system between the headquarters and the regional units, this step may be helpful. On the other hand, this proposal represents a clear move towards strong centralisation of crisis management. In countries such as the Czech Republic and Poland, where the security system works efficiently, this is due to decentralisation. Regional authorities in the Czech Republic and voivodeships in Poland serve as active mediation units, bridging potential disputes or ambiguities between headquarters and local governments. In contrast, the Slovak security system is more linear, with a greater number of direct links, which repeatedly overloads the central authorities, and this move emphasises precisely this linearity by reinforcing the concentration of competences, information and capacities exclusively at the central level.

At the same time, *the weak digitalisation of the security system* represents another **weakness** of the Security System of the Slovak Republic. The absence of modern tools for sharing information between the system components slows down the security system's response during crises. In Poland, it was the National Digital Platform that enabled rapid communication with citizens and effective coordination. The Czech Republic introduced an online portal for crisis management that integrated regional and central data. This portal served as a central point for sharing information between the government, regional authorities and the public. It allowed monitoring the current epidemiological situation, the measures taken and provided guidance for citizens and businesses. The integration of data from different levels of government ensured consistency of information and coordination of actions across the country what minimised confusion and improved the effectiveness of the pandemic response. (Crisis portal, 2022)

The introduction of a modern digital platform as proposed in the New Security System Concept would address this weakness. The current (2024) Minister of the Interior's proposal for a new comprehensive framework of processes and procedures for crisis management partially addresses the lack of digitalisation and the absence of modern information sharing tools, as it includes a plan for mapping and updating assets for crisis prevention, prevention and management and the development of information systems (Proposal for a new comprehensive framework of processes and procedures for crisis management in the Slovak Republic, 2024; The Ministry of Interior of the Slovak Republic, 2024).

Another **weakness** of the Slovak security system is *the investment debt in technology and infrastructure, as well as financial constraints, which are mainly manifested at the local level*. Even the 2021 Security Strategy of the Slovak Republic emphasised funding as a key factor for the sustainability and effectiveness of the security system and identifies it as an essential prerequisite for ensuring the Slovak Republic's ability to face security challenges, such as military threats, hybrid attacks, cyber security or crisis management, while pointing to the need for long-term, stable and predictable financing of the security system to cover the costs of building and modernising critical infrastructure, technological development in areas such as cyber security and digitalisation, and prevention and preparation for managing emergencies (Security Strategy of the Slovak Republic, 2021). Increasing spending in the security area is necessary both in the context of military security and defence, where Slovakia needs to fulfil, among other things, its commitments to the North Atlantic Alliance (2% of GDP to the country's defence capability), but also in the context of non-military security, where the financing of non-military components of civil protection of crisis management is crucial. In addition, the Security Strategy of the Slovak Republic identifies the need for better funding at local and regional levels, particularly in the area of crisis management. It proposes the creation of crisis funds to support local governments in dealing with emergencies such as floods, forest fires and pandemics. The consequences of insufficient funding in this area could be seen, for example, during the 2024 floods, when some municipalities did not have sufficient resources on their own to provide for evacuation and recovery. Slovakia also needs to invest more in advanced technologies to improve response to hybrid and cyber threats and to support research and development in the field of security. At the same time, Slovakia should reduce the burden on the public budget, in particular by strengthening its participation in international programmes from the EU and NATO, such as the European Defence Fund (EDF) to support technological and defence innovation and the RescEU to finance civil protection measures (Security Strategy of the Slovak Republic, 2021).

The Ministry of Interior's ambitious plan to first map the actual situation and assets in the field of crisis management as part of the project to create an Office for Crisis Management (OCM) is therefore a much-needed step, but what is questionable is the subsequent ability to secure funding for the elimination of the investment debt and, of course, the funding of the created entity and its further development.

### 4.3 Opportunities

Among the **opportunities**, and in relation to the above, we could also mention *the digitalization of the security system*, which offers the opportunity for better monitoring and prediction of threats, the ability to respond also to cyber security threats and the opportunity to shorten response times through digitalisation. The Security Strategy of the Slovak Republic 2021 addresses digitalization of the security system as a key tool for increasing the efficiency, flexibility and resilience of the Slovak security system. The document identifies digitalization as one of the strategic objectives for coping with modern threats, including cyber-attacks, hybrid threats and the need for rapid coordination between the components of the security system. The draft New Security System Concept also recommends investing in cyber security and digital solutions. The Programme Declaration of the Government of the Slovak Republic for 2023 - 2027 emphasises the digitalization of public administration as one of the main priorities (New Concept of the Security System of the Slovak Republic, 2023). The Government is committed to developing an efficient public administration. (Programme Statement of the Government of the Slovak Republic, 2023) And although the currently proposed comprehensive framework of processes and procedures for crisis management of the Slovak Republic from the Ministry of the Interior does not yet respond to this need, the government also plans to strengthen the material and technical support and staffing of all components of the Ministry of the Interior, which will encourage the effective digitalization of public space. (Office of the Government of the Slovak Republic, 2024) Currently, there are many calls, funded by the Programme Slovakia or the EU Recovery and Resilience Plan, which are focused on partial objectives, such as supporting regional public administration in the field of cyber and information security. While such challenges will not ensure a comprehensive digitalization of the security system, in the long term they will help to improve the quality of services provided by public administrations and ensure compliance with legislative requirements in the field of cyber and information security. (Ministry of Investments, Regional Development and Informatization of the Slovak Republic, 2024) In the long term, it is essential to follow the example of the Czech Republic and Poland, where digital platforms have enabled better coordination and rapid information exchange in crisis management.

Another **opportunity** for the development of the Slovak security system is *the development of international cooperation*, which, thanks to cooperative security mechanisms and the sharing of experience, procedures and security capabilities, helps Slovakia to gain greater resilience to threats. The Security Strategy of the Slovak Republic 2021 underlines the need to align Slovak crisis mechanisms with international standards to ensure a high level of preparedness. In this context, it mentions, for example, the strengthening of cooperation with NATO in the framework of *the Civil Emergency Planning Committee* and the use of EU civil protection mechanisms, mandatory participation in joint NATO-EU exercises simulating various crisis scenarios (e.g. natural disasters, pandemic threats, cyber-attacks). The Security Strategy of the Slovak Republic also stresses the importance of joint operations to increase interoperability between Slovak forces and international partners. The international cooperation in protecting critical infrastructure from cyber and hybrid threats is also a key priority. It is important for Slovakia to participate in projects such as the *NATO Cooperative Cyber Defence Centre of Excellence* with the possibility to use the expertise of EU member states. The Security Strategy of the Slovak Republic also emphasises the importance of bilateral cooperation with neighbouring states in dealing with cross-border crises, as well as the need for a coordinated approach to securing supplies of strategic materials (e.g. medical supplies, food) through international partners. In the area of international cooperation in crisis management, the Programme Declaration of the Government of the Slovak Republic for 2023 - 2027 focuses on strengthening partnerships with international organisations such as NATO and the European Union. Slovakia plans to continue its active participation in European Union initiatives such as RescEU, which provides resources and capacities to manage major crises (natural disasters, pandemics). In the NATO area, the importance of exercises and joint operations that improve interoperability and preparedness for both military and civilian crisis situations is highlighted. The need to deepen cooperation with neighbouring countries, in particular within the Visegrad Four (V4), is highlighted. This cooperation should include coordination in crisis planning, sharing of best practices and the creation of joint response units. The Government of the Slovak Republic aims to make active use of regional security mechanisms to support Slovakia in major crisis situations. The Programme Declaration emphasises international training programmes and exchange of experience, especially in the areas of hybrid threats, cyber security and crisis management. (The Programme Declaration of the Government of the Slovak Republic, 2023) Both documents agree on the need for cross-border cooperation and building interoperability, with the Security Strategy of the Slovak Republic placing more emphasis on digitalization and hybrid threats, while the Programme Declaration reflects regional cooperation and exchange of experience within the V4. At the same time, the project currently under preparation for a central Crisis Management Office at the Ministry of the Interior sees international cooperation not only as an opportunity but also as an obligation to fulfil the commitments associated with this cooperation. It emphasises the need to describe the current state of play, to propose a new model for the future functioning of crisis management that will meet current national as well as supranational requirements (NATO Resilience Committee, etc.) in this area, to prepare changes in the relevant legislation, to create a new entity and to put it into operation (with particular emphasis on the organisational structure, but also on staffing, financial resources and budget, priorities, objectives, programme management). According to the Ministry of the Interior of the Slovak Republic, the creation and implementation of such a comprehensive framework for risk management, damage and consequence reduction is also one of the priorities of the Government of the Slovak Republic and a requirement of our partners and allies in supranational organisations (NATO, EU). (Proposal for a new comprehensive framework of processes and procedures for crisis management in the Slovak Republic, 2024; The Ministry of Interior of the Slovak Republic, 2024)

*The unification of crisis planning methodologies* can also be **an opportunity** for the security system, ensuring better coordination of responses at all levels and speeding up the ability to respond to incoming threats, thanks to clear rules for all actors. **L. Šimák** (2016) highlights the importance of a systematic approach to the identification and analysis of risks that may threaten public administration and society as a whole. He proposes the implementation of comprehensive strategies to manage crisis situations, emphasizing the need for coordination between different levels of public administration and other stakeholders, the creation of a unified crisis planning methodology to ensure effective cooperation and communication between the different components of the system. This approach should include a clear definition of competences and responsibilities, the identification of roles for each entity involved in crisis management, standardised procedures and processes to help establish a set of uniform guidelines and protocols for dealing with crisis situations, and the implementation of regular training and exercises to ensure the preparedness of human resources through continuous education and practical drills. According to Šimák, the implementation of these measures would contribute to increasing the resilience of the public administration to crisis phenomena and ensure effective management of emergencies in the conditions of the Slovak Republic (Šimák, 2016).

The recommendation of a unified methodology of crisis planning was also brought by the draft of the new concept of the security system of the Slovak Republic from 2023. The proposal of the Ministry of the Interior of February 2024 to establish the Office for Crisis Management (OCM) directly responds to the need for the introduction of a unified crisis planning methodology. The aim of the forthcoming project is to precisely improve coordination between all levels of management. The establishment of the Office for Crisis Management is intended to ensure a unified approach to crisis planning and management within the Slovak Republic. The Office will be responsible for the entire crisis management cycle, including prevention, preparation, crisis management and recovery. This will remove the current legislative, personnel and material and technical shortcomings that have made it difficult to manage crisis situations effectively. (Proposal for a new comprehensive framework of processes and procedures for crisis management in the Slovak Republic, 2024; The Ministry of Interior of the Slovak Republic, 2024)

At this point, however, it should be pointed out again that while Slovakia is moving towards centralisation of crisis management through the OCM, the Czech Republic and Poland favour decentralised models. In the Czech Republic, crisis management is organised at regional level, with regional authorities playing a key role in the coordination and implementation of measures. This approach allows for a more flexible response to local specificities and needs (Act No. 240/2000 Coll., on Crisis Management). The Polish voivodeships (regional authorities) also have considerable autonomy in managing crisis situations, which allows for the adaptation of measures to local conditions and more effective cooperation with local authorities. (Urbanek, 2014) Slovakia has chosen a centralised model of crisis management due to the experience of recent years, which revealed legislative, personnel, material and technical shortcomings in dealing with emergencies. The centralisation is intended to ensure the uniform procedures and coordination at the national level, thus avoiding a confusion and duplication of competences.

## 4.4 Threats

**Threats** could include *the asymmetric security threats* such as *hybrid and cyber threats*, as well as *low public awareness and financial constraints*, as it was mentioned above.

A low public awareness is particularly problematic in the context of declining public trust in public institutions and the subsequent measures they take. This was evident during the COVID-19 pandemic, when a lack of public information caused confusion and reduced confidence in the measures taken. In general, if the state is not transparent enough and does not inform the public sufficiently about security actions that affect the public, the public loses trust and may start to disrespect the regulations. In the Czech Republic, it was the awareness campaigns that helped to systematically build public trust in the state. (Ministry of the Interior of the Czech Republic, 2024) Also, the draft of the New Concept of the Security System of the Slovak Republic recommends to strengthen awareness campaigns that would not cause panic and would not cause unnecessary fear, but would bring the public closer to the issue of security threats and the possibilities that the state has to eliminate them in order to protect the public from their unwanted effects. This is especially true if the threats in question are new, unusual, atypical or asymmetric in nature. Such threats require a particularly sensitive form of communication to the public. The Slovak Republic launched the portal hybridnehrozby.sk and implemented at the level of the Ministry of the Interior of the Slovak Republic in cooperation with the Police Force of the Slovak Republic an awareness campaign "Hoaxy sa na mňa nelepia“ *(Hoaxes don't stick to me),* the continuation of which after the change of government cannot be documented. Officially, this campaign has not been terminated, but it is not active and the social networks that were used for this purpose are still active but do not declare a link to the Ministry of the Interior of the Slovak Republic. The web portal hybridnehrozby.sk is still active with the operator of the Centre for Countering Hybrid Threats of the Ministry of the Interior and the Ministry of the Interior of the Slovak Republic, the Ministry of Foreign and European Affairs of the Slovak Republic, the Office of the Government of the Slovak Republic, the Ministry of Defence of the Slovak Republic, the Academy of the Police Corps as partners of the project. It is also a project implemented from the Effective Public Administration Operational Programme from the European Social Fund of the EU.  General information such as Basic Conceptual and Strategic Documents on Hybrid Threats and information on foreign events, and articles and analyses as early as 2023 are available on the website (Centre for Countering Hybrid Threats of the Ministry of Interior of the Slovak Republic, 2024).

We consider *hybrid and cyber threats* as another **threat** in the SWOT analysis of the security system of the Slovak Republic. The Security Strategy of the Slovak Republic of 2021 identifies hybrid and cyber threats as significant risks to national security. The document emphasises the need to strengthen the resilience of the state and society to these threats, including disinformation, and to ensure a functional cyber, information and communication security system. The 2023 draft of the new concept of the security system of the Slovak Republic identifies hybrid and cyber threats as significant risks to national security. The document emphasises the need to improve the efficiency of the state security system without creating new institutions, with the focus of increasing resilience being on the coordination of individual entities through the activities of the Security Council of the Slovak Republic. Particular emphasis is placed on streamlining the work of the committees of the Security Council of the Slovak Republic and strengthening the competences of the Director of the Security Council Office (New Concept of the Security System of the Slovak Republic, 2023).

In accordance with the Action Plan for Coordinated Countering of Hybrid Threats 2022 - 2024, the process of establishing *the Committee on Hybrid Threats*, which was established as a permanent working body of the Security Council of the Slovak Republic, was ongoing. Its task is to coordinate the planning of measures to maintain security and build the Slovak Republic's resilience to hybrid threats. This committee was established by the amendment to Act No. 110/2004 Coll. on the Activity of the Security Council of the Slovak Republic at the Time of Peace, which entered into force in May 2023. The cooperation of this specialised committee with other committees of the Security Council of the Slovak Republic is intended to contribute to linking the sharing of information on specific security threats with the threats already defined in *the National Security Threat Risk Management Strategy of the Slovak Republic* (hereinafter also as “Strategy”), which identifies hybrid threats as a serious risk to the stability and security of Slovakia, citing the need for a multidisciplinary and multi-agency approach. This includes cooperation between the public and private sectors, including the active involvement of private companies, academic community and the civil sector; the sharing of information and experience between government departments and international partners and the establishment of an integrated information system to monitor threats and coordinate responses. The cyber threats are described as a growing risk that requires specific strategies and actions. According to the Strategy, the key actor in this area is the National Security Office (NSO). The Strategy highlights the need to establish digital platforms for information sharing and coordination of responses to cyber security incidents. Public-private partnerships and the modernisation of technological infrastructure are seen as key elements to increase resilience to cyber-attacks. The Strategy also stresses the importance of education and awareness-raising on hybrid and cyber threats among the public and professionals. In general, the document identifies the need to expand and strengthen national capabilities, in particular by creating a unified framework for risk assessment, strengthening technical infrastructure and investment in cyber security, and ensuring coordination between crisis management components at both national and regional levels. (National Security Threat Risk Management Strategy of the Slovak Republic, 2023) Given the need to respond to hybrid threats, the Centre for Countering Hybrid Threats was established at the level of the Ministry of the Interior, which is an organisational component of the Ministry of the Interior within the Institute of Administrative and Security Analysis. Its main objective is to increase Slovakia's preparedness and resilience to various forms of hybrid threats, such as disinformation, cyber-attacks or corruption.  It monitors and assesses potential threats in the media and digital environment, assesses existing legal and organizational frameworks to identify vulnerabilities and suggest improvements, develops recommendations to strengthen the state's resilience to hybrid threats, organizes training and simulation sessions for public administration employees and other relevant entities to enhance their preparedness. It also cooperates with international partners, including the European Centre of Excellence for Countering Hybrid Threats (hereinafter also as “the Centre”), where Slovakia is one of 31 member countries. In September 2023, the Centre launched the website www.hybridnehrozby.sk, which provides comprehensive information on hybrid threat issues for the general and professional public, and an awareness campaign, Hoaxy sa na mňa nelepia (Hoaxes Don't Stick to Me), was also launched. The Centre is still active and continues its activities, focusing on identifying, analysing and addressing hybrid threats to strengthen the security and resilience of the Slovak Republic (Centre for Countering Hybrid Threats of the Ministry of Interior of the Slovak Republic, 2024).

The Programme Declaration of the Government of the Slovak Republic of 2023 focuses on improving the security environment, but specific measures regarding hybrid and cyber threats are not explicitly mentioned in the available parts of the document. Similarly, the 2024 draft of a new comprehensive framework of processes and procedures for crisis management by the Ministry of the Interior proposes the establishment of an Office for Crisis Management (OCM) to centralise crisis management in Slovakia, but it primarily focuses on improving coordination in crisis situations and does not include specific measures on hybrid and cyber threats (the Programme Declaration of the Government of the Slovak Republic, 2023; Office of the Government of the Slovak Republic, 2024).

Also, the aforementioned *Committee on Hybrid Threats* was established as a permanent working body of the Security Council of the Slovak Republic. However, according to the information available as of August 2023, it appears that the Committee has not yet met, as there is no mention of the Committee's work plan in the 2024 Work Plan of the Security Council of the Slovak Republic. (Security Council of the Slovak Republic, 2024)

From this point of view, it can be stated that the biggest threat to the security system of the Slovak Republic is the fact that the Slovak Republic does not have a strategic approach to the issue of hybrid threats at the top level of state management, either within the Security Council of the Slovak Republic or at the government level.

In the event that a security threat of hybrid or cyber origin needs to be eliminated, the Slovak Republic addresses these threats on the basis of ad hoc proposals from individual ministries, as we have seen in the case of the cyber threat through e-mail threats of bomb attacks on schools. In recent months, the security system of the Slovak Republic has faced a series of bomb threats sent via e-mail to hundreds of schools across the country. These incidents prompted an immediate and coordinated response by the relevant authorities to ensure the safety of pupils and staff. Following the receipt of the threatening e-mails, the schools concerned were evacuated and the premises were searched by police forces to verify the presence of explosives. For example, in May 2024, approximately 1,544 such threats were registered, none of which were confirmed after thorough searches. (Pravda, 2024) 2,050 police officers were allocated to provide security, with each school having a police officer assigned to it who could be contacted at any time. The police opened a prosecution for the particularly serious crime of terrorist attack. If proven guilty, the perpetrator faces a maximum sentence of 25 years imprisonment or an exceptional sentence of life imprisonment. (Pravda, 2024) As similar threats have been reported in other countries, the Slovak authorities have worked with international partners to identify perpetrators and coordinate security measures. (Körtvélyesiová, ,2024) The Ministry of Education, Research, Development and Youth of the Slovak Republic has provided schools with guidelines on how to deal with bomb threats, including evacuation plans and communication with parents. (Ministry of Education, Research, Development and Youth of the Slovak Republic, 2024) As threats were sent electronically, measures to monitor and prevent cyber-attacks were strengthened, including cooperation with the National Security Bureau and other relevant institutions. (Hospodárske noviny, 2024)

The Security System of the Slovak Republic responded to the bomb threats in a prompt and coordinated manner, taking measures to protect the population and minimise disruption to the educational process. At the same time, it focused on identifying the perpetrators and strengthening preventive measures to avoid similar incidents in the future.

Subsequently, the Minister of the Interior presented the concept of strengthening school security through the installation of CCTV cameras. An analysis of public facilities where increased surveillance and protection is needed showed the greatest need for them at schools. A pilot project is expected to be implemented at three selected schools in the coming months. The main objective of installing CCTV systems is to increase control over access to school buildings and to monitor the movement of people around the schools. These systems will not only reduce the risk of unauthorised access, but will also provide an important tool for rapid response in the event of a security incident. This security system is intended to help prevent hybrid threats in the school environment, such as the bomb threats just mentioned. (The

Ministry of Interior of the Slovak Republic, 2024) On the other hand, the Minister of Interior has not yet offered an expert argument when asked how CCTV systems will help stop the sending of bomb threat emails.

As similar attacks were happening in the Czech Republic at the same time, we provide a comparison of the responses:

Response in the Slovak Republic:

- Evacuation of schools - following the receipt of threatening emails, several schools were evacuated to ensure the safety of pupils and staff. The Slovak police subsequently carried out searches of the premises.
- Disruption of classes - in some cases classes were cancelled, disrupting the educational process and causing complications for parents and students
- Ensuring information - setting up a sub-page on the Ministry of Education, Research, Development and Youth's website where schools had all relevant information in one place, with the abovementioned ministry advising schools to shorten classes.

Response in the Czech Republic:

- Minimising disruption to teaching – the Czech police took measures to interfere as little as possible with the teaching regime. The aim was to maintain the continuity of education and minimise panic among students and parents.
- Focus on investigation – the Czech police forces concentrated on identifying the origin of the threats and worked with international partners to identify the perpetrators.
- Ensuring awareness – the Czech police communicated extensively with school representatives and took appropriate action, while trying to interfere as little as possible with the normal running of schools. The aim was to ensure continuity of education and avoid unnecessary panic.

From a brief comparison, we can identify at least the following shortcomings. Many evacuations and disruptions in Slovakia have led to considerable disruption of the educational process, especially in comparison with the Czech Republic, where the priority has been to maintain the continuity of classes. The repeated evacuations in Slovakia may have increased the level of fear and panic among those affected, for which the above-mentioned camera system is supposed to be **an improvised solution**, but it does not represent a comprehensive solution and raises many questions and uncertainty on the part of those affected. In the Czech Republic, on the other hand, the emphasis has been on investigating the origin and source of the bomb threats on the one hand, and on keeping the peace and minimising interference in the normal running of schools on the other.

### Summary of the analysis of the security system of the Slovak Republic

In terms of strengths, we can state that the Security System of the Slovak Republic has a comprehensive legislative framework that enables crisis management at various levels. We can also consider the links with supranational structures such as NATO and the EU and, last but not least, the fact that the Security System of the Slovak Republic also applies the principle of subsidiarity, i.e. it involves local state and municipal authorities in crisis management.

In terms of weaknesses, we can speak in particular about the fragmentation of competences between the central, regional and local levels of the Slovak security system management. Weaknesses also include the lack of digitisation of the security system and the absence of modern information sharing tools. Also problematic is the insufficient allocation of funding for crisis management at the level of municipalities, which reduces their ability to respond immediately to or prevent these incoming threats.

In terms of opportunities, if the lack of digitalisation is a weakness of the Slovak security system, then greater digitalisation and the creation of digital platforms to support crisis management is, on the contrary, an opportunity. A deepening and strengthening of the strengths in international cooperation, critical infrastructure protection and crisis management is also a great opportunity for Slovakia. We see the same opportunity after the implementation of the unified crisis planning methodology. A unified legislative framework would bring room for improvement in all areas of security system management.

The biggest current threats to the security system are, firstly, the low public awareness of security issues, secondly, without a doubt, the increasing rise of hybrid and cyber threats that threaten the infrastructure and stability of the security environment in Slovakia, and last but not least, problematic funding, as the lack of resources for prevention and response weakens the overall capacity of the security system as a whole. The currently planned steps presented by the Ministry of the Interior of the Slovak Republic also objectively show the risk of inefficient centralisation of crisis management.

## 5. Recommendations for practice

In order to improve the efficiency of the Slovak security system, it is necessary to introduce several concrete measures. In the area of legislation, it is crucial to unify the existing legal norms related to crisis management and security policy into one comprehensive framework. This consolidation would eliminate duplication and ensure a consistent approach to security threat management. It is also important to implement a single crisis planning methodology that would serve as a standard for all levels of government, thereby improving the coordination and effectiveness of responses.

A digitalization is another area that requires significant investment. The creation of modern digital platforms for sharing information between the different components of the security system would allow for fast and efficient communication during crisis situations. At the same time, there is a need to strengthen capacities in the field of cyber security and protection against hybrid threats, which requires not only technological investment but also systematic training of personnel.

A funding plays a crucial role in the security system. The introduction of crisis funds, which would provide local and regional governments with resources to deal with unexpected events, would significantly improve their ability to respond to crisis situations. At the same time, there is a need to increase the budget for crisis prevention and preparedness, especially at local government level, which often faces the direct consequences of emergencies.

At international level, Slovakia should deepen cooperation with NATO and EU allies, especially in the area of hybrid and cyber threats. Regional partnerships within the Visegrad Four can also bring synergies in crisis management. A key step is the exchange of best practices and participation in joint exercises that enhance interoperability and preparedness.

Finally, it is essential to strengthen education and awareness-raising. Regular training of public servants and informing the public about their roles during crisis situations will increase the preparedness of society as a whole. At the same time, it is necessary to promote public debate on security issues and to raise awareness of current threats and how Slovakia can respond effectively to them. This comprehensive approach will ensure a more resilient security system and its ability to face current and future challenges.

## Conclusion

The assessment of the effectiveness of the Slovak security system shows that despite a robust legislative framework and membership in international organisations such as NATO and the EU, the system faces a number of challenges that limit its ability to respond effectively to current threats. Fragmentation of competences between different levels of government and shortcomings in the digitalization of crisis management are the main weaknesses undermining coordination and the speed of responses to crisis situations. At the same time, hybrid and cyber threats are on the rise, increasing pressure to improve system resilience and integrate modern technologies.

On the other hand, the implementation of a common methodology for crisis planning, the strengthening of digitalization and the use of best practices from international practice provide significant opportunities for development. Examples from the Czech Republic and Poland show that a decentralised approach, reinforced by an efficient digital infrastructure, can lead to more flexible and faster crisis management.

In order to ensure a more efficient functioning of the Slovak security system, it is essential to implement the recommendations of the New Security System Concept, in particular in the areas of digitalization, hybrid threats and strengthening cooperation between all levels of government. By focusing on these aspects, Slovakia can increase its preparedness and resilience to modern threats and improve the protection of citizens and critical infrastructure.

## References

*Bezpečnostná stratégia SR*. 2001 [online]. Národná rada SR. [cit. 2024-11-10]. Available at: https://www.nrsr.sk/web/Dynamic/Download.aspx?DocID=458853 *(Security Strategy of the Slovak Republic, 2001)*

*Bezpečnostná stratégia SR.* 2005 [online]. Ministerstvo obrany SR. [cit. 2024-11-10]. Available at: https://www.mosr.sk/data/files/4264_bezpecnostna-strategia-sr-2005.pdf *(Security Strategy of the Slovak Republic, 2005)*

*Bezpečnostná stratégia SR*. 2021. [online]. Ministerstvo obrany SR. [cit. 2024-11-10]. Available at: https://www.mosr.sk/data/files/4263_210128-bezpecnostna-strategia-sr-2021.pdf *(Security Strategy of the Slovak Republic, 2021)*

*Bombové hrozby na školách boli pravdepodobne kybernetický útok, potvrdila polícia*. 2024. [online] TASR. Hospodárske noviny. [cit. 2024-10-9]. Available at: https://hnonline.sk/slovensko/96148222-bombove-hrozby-na-skolach-boli-pravdepodobne-kyberneticky-utok-potvrdila-policia *(Hospodárske noviny, 2024)*

BREZINA, D., 2022. *Rozhodovacie procesy na nižších úrovniach krízového riadenia*. Liptovský Mikuláš: Akadémia ozbrojených síl generála M. R. Štefánika, ISBN 978-80-8040-616-5

BUZALKA, J., 2012. *Krízový manažment vo verejnej správe*. Bratislava: Akadémia PZ. ISBN 978-80-8054-527-7.

*Centrum boja proti hybridným hrozbám MV SR*. 2024 [online]. Centrum boja proti hybridným hrozbám. [cit. 2024-10-9]. Available at: https://www.hybridnehrozby.sk/ *(Centre for Countering Hybrid Threats of the Ministry of Interior of the Slovak Republic, 2024)*

*COVID AUTOMAT*. 2021. [online] Ministerstvo zdravotníctva SR [cit. 2024-10-10]. Available at: https://www.minv.sk/swift_data/source/images/020221%20COVID%20automat%20Signalizacny%20system%201v4.pdf *(Ministry of Health of the Slovak republic, 2024)*

*Dezinformační kampane.* 2024 [online]. Ministerstvo vnitra ČR. [cit. 2024-10-9]. Available at: https://www.mvcr.cz/clanek/dezinformacni-kampane.aspx?utm_source=chatgpt.com *(Ministry of Interior of the Czech Republic, 2022)*

HOFREITER, L., BREZINA D., 2023 *Bezpečnosť, bezpečnostná politika a bezpečnostný systém*. Liptovský Mikuláš: Akadémia ozbrojených síl generála M. R. Štefánika. 2023. ISBN 978-80-8040-657-8.

*Informace o speciálních stránkách HZS CR ke koronaviru*. 2022. [online]. Krizový portál. [cit. 2024-10-9]. Available at: https://www.krizport.cz/aktualni-situace/aktuality/all-informace-o-specialnich-strankach-hzs-cr-ke-koronaviru *(Crisis portal, 2022)*

KÖRTVÉLYESIOVÁ, D., 2024. *Slovenská vláda reaguje na bombové hrozby: Prezradili detaily útokov a jasné odporúčania pre školy.* [online] Tlačová správa Úradu vlády SR. [cit. 2024-10-9]. Available at: https://www.startitup.sk/slovenska-vlada-reaguje-na-bombove-hrozby-prezradili-detaily-utokov-a-jasne-odporucania-pre-skoly-navod

*Košický samosprávny kraj pomáha zabezpečiť priestory a zdravotníkov na celoplošné testovanie.* 2020. [online]. Košický samosprávny kraj. [cit. 2024-10-9]. Available at: https://web.vucke.sk/sk/novinky/kosicky-samospravny-kraj-pomaha-zabezpecit-priestory-zdravotnikov-celoplosne-testovanie.html *(Košice Self-Governing Region, 2022 and 2022)*

LUŽÁK, J., KLAČKO, L., 2019. *Audit bezpečnostného systému SR* [online]. Globsec. [cit. 2024-10-9]. Available at: https://www.globsec.org/sites/default/files/2019-09/Audit-Bezpecnostneho-Systemu-SR-v-kontexte-HH.pdf

MIHALKOVÁ, H., LAUKOVÁ, L., 2024. *Každá škola dostala svojho policajta. Vinníkovi za teroristické bombové vyhrážky hrozí aj doživotie*. [online]. Denník Pravda [cit. 2024-10-9]. Available at: https://spravy.pravda.sk/domace/clanok/709303-kazdy-skola-dostala-svojho-policajta-vinnikovi-za-teroristicke-bombove-vyhrazky-hrozi-aj-dozivotie/

*Ministerstvo školstva odporučilo školám postihnutým bombovou hrozbou skrátiť vyučovanie*. 2024. [online]. Ministerstvo školstva, vedy, výskumu, vývoja a mládeže SR. [cit. 2024-10-9]. Available at: https://www.minedu.sk/ministerstvo-skolstva-odporucilo-skolam-postihnutym-bombovou-hrozbou-skratit-vyucovanie/ *(Ministry of Education, Research, Development and Youth of the Slovak Republic, 2024)*

*Na Slovensku vzniklo pre verejnosť 88 očkovacích centier, z toho 14 veľkokapacitných.* 2021. [online]. Ministerstvo zdravotníctva SR. [cit. 2024-10-10]. Available at: https://www.health.gov.sk/Clanok?covid-19-14-03-2021-ockovacie-centra *(Ministry of Health of the Slovak republic, 2024)*

*Národná stratégia riadenia rizík bezpečnostných hrozieb Slovenskej republiky.* 2023. [online]. Úrad vlády SR. [cit. 2024-10-9]. Available at: https://rokovania.gov.sk/RVL/Material/26865/1 *(National Security Threat Risk Management Strategy of the Slovak Republic, 2023)*

*Návrh nového komplexného rámca procesov a postupov pre krízové riadenie Slovenskej republiky*. 2024. [online]. Úrad vlády SR. [cit. 2024-10-9]. Available at: https://rokovania.gov.sk/RVL/Material/29227/1 *(Proposal for a new comprehensive framework of processes and procedures for crisis management in the Slovak Republic, 2024)*

*Nová koncepcia bezpečnostného systému SR*. 2005. [online]. Úrad vlády SR. [cit. 2024-11-10]. Available at: https://rokovania.gov.sk/RVL/Material/28141/1 *(New Concept of the Security System of the Slovak Republic, 2023)*

*Nová výzva podporí subjekty verejnej správy v oblasti kybernetickej a informačnej bezpečnosti*. 2024 [online] Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky [cit. 2024-10-9]. Available at: https://mirri.gov.sk/aktuality/digitalna-agenda/nova-vyzva-podpori-subjekty-verejnej-spravy-v-oblasti-kybernetickej-a-informacnej-bezpecnosti/ *(Ministry of Investments, Regional Development and Informatization of the Slovak Republic, 2024)*

*Pandemický plan ČR*. 2022.[online]. Ministerstvo zdravotnictví ČR [cit. 2024-10-9]. Available at: https://mzd.gov.cz/category/ochrana-verejneho-zdravi/pandemicky-plan-cr/ *(Ministry of Health of the Czech Republic, 2022)*

*Plán práce Bezpečnostnej rady Slovenskej republiky na rok 2024.* 2024. [online]. Úrad vlády SR. Kancelária Bezpečnostnej rady SR. [cit. 2024-10-9]. Available at: https://www.vlada.gov.sk/site/assets/files/1765/pla_n_pra_ce_br_sr_na_rok_2024.pdf *(Security Council of the Slovak Republic, 2024)*

*Programové vyhlásenie Vlády Slovenskej republiky na obdobie rokov 2021-2024*. 2021. [online]. Národná rada SR. [cit. 2024-10-9]. Available at: https://www.nrsr.sk/web/Dynamic/DocumentPreview.aspx?DocID=494677 *(Programme Statement of the Government of the Slovak Republic, 2021)*

*Programové vyhlásenie Vlády SR na obdobie rokov 2023-2027*. 2024. [online]. Národná rada SR. [cit. 2024-10-9]. Available at: nrsr.sk/web/Dynamic/DocumentPreview.aspx?DocID=535376 *(Programme Statement of the Government of the Slovak Republic, 2024)*

PROKOPČÁKOVÁ, D., 2024. *Populizmus, ignorácia odborníkov a slabý boj s dezinformáciami. Ako sme (ne)zvládli pandémiu.* [online]. [cit. 2024-10-9]. Available at: *https://primar.sme.sk/c/23396074/pandemia-slovensko-hodnotenie-odbornici.html*

ŠIMÁK, L., 2016*. Krízový manažment vo verejnej správe.* Druhé prepracované vydanie. Žilina: EDIS - vydavateľské centrum ŽU. ISBN 978-80-554-1165-1.

*Štatút Bezpečnostnej rady Slovenskej republiky*. 2024. [online] Úrad vlády SR. [cit. 2024-10-9]. Available at: https://www.vlada.gov.sk/site/assets/files/1765/s_tatu_t_u_lohy_kbr.pdf *(Statute of the Security Council of the Slovak Republic, 2024)*

URBANEK, A., 2014. Vybrané prvky systému národnej bezpečnosti Poľskej republiky. *Krízový manažment.* 1, pp. 73-80. [online]. [cit. 2024-10-9]. Available at: https://krm.uniza.sk/pdfs/krm/2014/01/13.pdf

UŠIAK, J., 2020*. Bezpečnostná politika Slovenskej republiky a vybrané bezpečnostné dokumenty*. Banská Bystrica: Belianum. ISBN 978-80-557-1795-1. 266s.

Ústava Slovenskej republiky č. 460/1992 Zb. (*Constitution of the Slovak Republic No. 460/1992 Coll.)*

Ústavný zákon č. 227/2002 Zb. o bezpečnosti štátu v čase vojny, vojnového stavu, výnimočného stavu a núdzového stavu (*Constitutional Act on State Security in Wartime, During Hostilities, Martial Law and State of Emergency No. 227/2002 Coll.*)

Uznesenie č. 110/2021 Z. z., Uznesenie vlády Slovenskej republiky č. 166 k návrhu aktualizácie mapy okresov podľa aktuálnej rizikovosti s ohľadom na šírenie ochorenia COVID-19. 2021. [online]. Zbierka zákonov SR. [cit. 2024-10-9]. Available at: https://www.epi.sk/zz/2021-110/znenie-20210329

*V očkovacom centre Košického samosprávneho kraja sa bude očkovať aj vakcínou od Moderny*. 2022. [online]. Košický samosprávny kraj. [cit. 2024-10-9]. Available at: https://web.vucke.sk/sk/novinky/v-ockovacom-centre-kosickeho-samospravneho-kraja-bude-ockovat-aj-vakcinou-od-moderny.html *(Košice Self-Governing Region, 2022 and 2022)*

*Vláda po dvoch desaťročiach prijala zásadné koncepčné zmeny v nastavení bezpečnostného systému štátu*. 2023 [online] Ministerstvo vnútra SR. [cit. 2024-10-9]. Available at: https://www.minv.sk/?tlacove-spravy&sprava=vlada-po-dvoch-desatrociach-prijala-zasadne-koncepcne-zmeny-v-nastaveni-bezpecnostneho-systemu-statu *(Ministry of Interior of the Slovak republic, 2024)*

*Vláda schválila koncepciu posilnenia bezpečnosti škôl prostredníctvom inštalácie kamerových systémov*. 2024. [online] Ministerstvo vnútra SR. [cit. 2024-10-9]. Available at: https://www.minv.sk/?tlacove-spravy&sprava=vlada-schvalila-koncepciu-posilnenia-bezpecnosti-skol-prostrednictvom-instalacie-kamerovych-systemov *(Ministry of Interior of the Slovak republic, 2024)*

*Všetko o téme hybridných hrozieb nájdete na novej webovej stránke hybridnehrozby.sk*. 2024. [online] Ministerstvo vnútra SR. [cit. 2024-10-9]. Dostupné z: https://www.minv.sk/?tlacove-spravy&sprava=vsetko-o-teme-hybridnych-hrozieb-najdete-na-novej-webovej-stranke-hybridnehrozby-sk *(Ministry of Interior of the Slovak republic, 2024)*

Zákon č. 110/2004 Z. z. o fungovaní Bezpečnostnej rady Slovenskej republiky v čase mieru, Bezpečnostná stratégia Slovenskej republiky (*Act No. 110/2004 Coll. on the Activity of the Security Council of the Slovak Republic at the Time of Peace)*

Zákon č. 240/2000 Sb. o krizovém řízení a o změně některých zákonů *(Act No. 240/2000 Coll. on Crisis Management and amending certain acts)*

Zákon č. 321/2002 Z. z. o ozbrojených silách Slovenskej republiky (*Act No. 321/2002 Coll. on the Armed Forces of the Slovak Republic and on Change and Amendment of Some Acts)*

Zákon č. 369/1990 Zb. o obecnom zriadení (*Act No. 369/1990 Coll. on Municipal Establishment)*

Zákon č. 387/2002 Z. z. o riadení štátu v krízových situáciách mimo času vojny a vojnového stavu *(Act No. 387/2002) Coll. on the Control of State in Crisis Situations Except for Wartime and During a State Hostilities)*

Zákon č. 42/1994 Z. z. o civilnej ochrane obyvateľstva (*Act No. 42/1994 Coll. on Civil Protection of Population and on amending and supplementing certain laws)*

Zákon č. 575/2001 Z. z. o organizácii činnosti vlády a organizácii ústrednej štátnej správy (*Act No. 575/2001 Coll. Code of Acts on Organization of Activities of the Government and Central Government as Amended).*

ŽÍDEK, R., CIBÁKOVÁ, S., 2009. *Bezpečnosť štátu.* Liptovský Mikuláš: Akadémia ozbrojených síl generálana M.R. Štefánika. ISBN 978-80-8040-375-1.

### Contact address

Mgr. Katarína Miňová, PhD.
ID ORCID: 0000-0002-5135-7427
Pavol Jozef Šafárik University in Košice
Faculty of Public Administration
Popradská 66, 040 22 Košice
Email: katarina.minova@upjs.sk