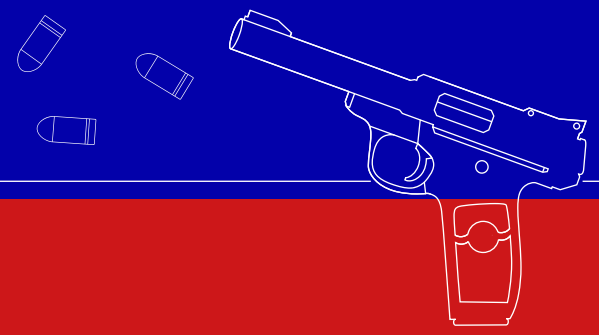
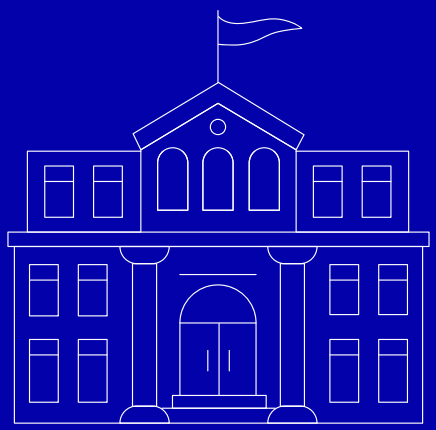
CENTRE
FOR COUNTERING
HYBRID THREATS



IN-DEPTH VULNERABILITY ANALYSIS OF SELECTED STATE ADMINISTRATION BODIES TO HYBRID THREATS

2023



MINISTRY
OF INTERIOR
OF THE SLOVAK REPUBLIC

Operational Programme
Effective
Public Administration

European Union
European Social Fund

Author: Centre for Countering Hybrid Threats, Institute of Administrative and Security Analyses of the Ministry of Interior of the Slovak Republic

Date of publication: August 2023

Centre for Countering Hybrid Threats
Institute of Administrative and Security Analyses
Ministry of Interior of the Slovak Republic
Pribinova 2
812 72 Bratislava
Slovak Republic

This publication has been produced with the financial support of the European Union. Its aim is to make available to the public information based on the non-public analytical material approved by the Security Council of the Slovak Republic by Resolution No. 818 at its meeting on 12 April 2023. The publication contains parts of the analysis in question, which identified the vulnerabilities of selected state administration bodies to hybrid action and proposed measures to eliminate them. This publication represents solely the views of the authors. The European Union is not responsible for the content or the views expressed in this publication.

National project "Increasing Slovakia's resilience to hybrid threats by strengthening public administration capacities". Project code in ITMS2014+: 314011CDW7

This project is supported by the European Social Fund.

This analysis is the result of a broad cooperation of the Centre for Countering Hybrid Threats of the Ministry of the Interior of the Slovak Republic with many units of the Ministry of the Interior, as well as with other institutional partners, without whom its elaboration would not have been possible. **Thank you!**

- Government Office of the Slovak Republic,
- Ministry of Foreign and European Affairs of the Slovak Republic,
- Ministry of Economy of the Slovak Republic,
- Ministry of Culture of the Slovak Republic,
- Ministry of Education, Science, Research and Sport of the Slovak Republic,
- Ministry of Investments, Regional Development and Informatization of the Slovak Republic,
- Ministry of Justice of the Slovak Republic,
- National Security Authority,
- Slovak Information Service,
- National Security Analytical Centre,
- Military Intelligence.

Table of contents

Introduction

“In the practical art of war, the best thing of all is to take the enemy's country whole and intact; to shatter and destroy it is not so good.“

Sun-Tzu, The Art of War

Disinformation, propaganda, cyber-attacks, influence and information operations, election interference, strategic corruption, paramilitary groups - all these terms have something in common. These are the most commonly used hybrid threat instruments. The term hybrid threats may be new, but the concept has been used for centuries. It consists in trying to weaken and incapacitate the opponent without deploying military forces.

The pursuit of one's own economic or geopolitical interests in international relations through diplomacy and other "soft" forms of engagement is a normal part of state-to-state relations. What distinguishes hybrid threats from these forms of international politics is the level of coordination between the various instruments and, in particular, the objective of such action. It is the incapacitation and disruption of society, or its security and governmental structures.

Hybrid threats have become one of the most important topics in security in recent years. In Slovakia as well as at the EU and NATO level. The reason why this area is given more and more importance is the change in the way strategic interests are pursued by hostile actors and the increasing impact of technology on all areas of society.

Warfare in the 21st century is being replaced by the coordinated use of a range of tools in the areas of information, economic influence, energy coercion and intelligence. At the same time, technology has become an integral part of the life of the entire society, and thanks to it, today hostile actors can operate anywhere in the world - spreading strategic propaganda, influencing electoral processes, attacking critical infrastructure, penetrating computer networks, etc.

The actors of hybrid threats are usually foreign hostile states whose political or strategic objectives are in conflict with the vital and strategic interests of the Slovak Republic and the organisations of which it is a member, such as the EU or NATO. Therefore, the activities of the Russian Federation are the most frequent in our conditions when dealing with hybrid threats. Russian Federation has even put Slovakia, along with other EU countries, on the list of hostile countries.[1]

[1] Government Regulation No. 1998-r of 22 July 2022 http://government.ru/en/docs/46080/ a Russian government approves list of unfriendly countries and territories - Russian Politics & Diplomacy - TASS.

Further, it is China that uses primarily economic forms and instruments. Such an assessment results both from the annual reports of the Slovak Information Service[2] or the Military Intelligence[3], as well as from documents adopted at the EU and NATO level[4]. Hybrid actors can also be non-state entities. A typical example is ISIS, which at the peak of its activities used several interconnected and coordinated tools in the field of information operations, cyber-attacks or terrorism.

Slovakia started working on increasing its resilience to hybrid threats as early as 2018, when the first *Concept for the Slovak Republic's Fight Against Hybrid Threats* was adopted[5]. The importance of this area has also been underlined in the current *Security Strategy of the Slovak Republic of 2021* and the most recent material in this area is the *Action Plan for the Coordinated Countering of Hybrid Threats* (hereafter referred to as "APHH") from 2022[6].

Understanding one's own vulnerabilities is the basis for successfully countering the threats posed by such covert, subversive hybrid threats to the strategic and vital interests of the Slovak Republic. For this reason, within the framework of the national project *"Increasing Capacities and Preparedness of the Slovak Public Administration for Hybrid Threats"*, there was a need to analyse the processes, structures and legislation of selected government entities in relation to possible hybrid actions. The result is the *In-Depth Analysis of the Vulnerabilities of Selected State administration bodies to Hybrid Threats* (hereafter referred to as the "In-Depth Analysis"), which is a reflection of Task A.1 resulting from the Action plan to coordinate the fight against hybrid threats.

This material is the result of extensive cooperation between the Ministry of the Interior of the Slovak Republic and a number of central government authorities and security services. The aim of the in-depth analysis was not only to identify vulnerabilities but also to propose measures to address them. The analysis includes an introductory chapter examining the overall system architecture for addressing hybrid threats within government, and 22 thematic chapters analysing vulnerabilities to specific hybrid threat instruments.

Due to the sensitivity of the information contained in the in-depth analysis, the material was approved at the meeting of the Security Council of the Slovak Republic by Resolution No. 818 on 12 April 2023 as classified material subject to the protection of classified information. The version you are holding is an edited version of this analysis for public distribution and discussion among the experts. It does not contain sensitive information, but still represents the most comprehensive mapping of vulnerabilities to hybrid threats, while offering concrete measures to address them.

[2] SIS Activity Report 2021 Slovenská informačná služba | Pre Vás | Správa o činnosti SIS (gov.sk).
[3] Military Intelligence Activity Report 2021 Sprava_o_cinnosti_vs_2021_svk.pdf (mosr.sk).
[4] The Russian Federation has been identified as the most significant and immediate threat to the security of the Allies as well as to peace and stability in the Euro-Atlantic area in NATO Strategickej koncepcie 2022, adopted at the Madrid Summit on 29 June 2022. At the EU level, the Strategický kompas, was adopted by the EU Council on 21 March 2022, identifying Russian threats, and the European Parliament deklaroval, in November 2022 that the Russian Federation is a state sponsor of terrorism and uses terrorist practices.
[5] Concept for Countering Hybrid Threats in the Slovak Republic, approved by Government Resolution No. 345/2018 on 11 July 2018 https://rokovania.gov.sk/RVL/Material/23100/1.
[6] Action Plan for the Coordination of Countering Hybrid Threats for the years 2022 to 2024, approved by Government Resolution No. 235/2022 of 30 March 2022.

Hybrid threat instruments

Hybrid actors can use different instruments in order to achieve their objectives. In identifying hybrid threat instruments, this analysis is based on a conceptual model developed within the EU's Joint Research Centre (hereinafter referred to as the „JRC"). The model developed by the JRC defines 40 hybrid threat instruments in 13 domains.

In the framework of this analysis, this model was adapted to the conditions of the Slovak Republic and the number of instruments was adjusted to 25. The instruments are ranked according to the identified risk from most to least severe:

1.	Disinformation campaigns and propaganda	**14.**	Pressure on politicians or members of the government
2.	Influencing elections	**15.**	Embassies
3.	Proliferation of weapons (including weapons of mass destruction)	**16.**	Using diasporas for influence
4.	Cyber operations - violation of confidentiality, integrity and availability in cyberspace	**17.**	Diplomatic and economic sanctions
5.	Physical operations against infrastructure	**18.**	Controlling and interfering with the media
6.	Promoting social unrest and exploiting socio-cultural cleavages	**19.**	Foreign direct investment
7.	Exploiting weaknesses in public administration	**20.**	Creating and exploiting infrastructure dependencies (energy, energy infrastructure and civil-military dependencies)
8.	Misuse of migration as a hybrid threat instrument	**21.**	Creating and exploiting economic hardship and dependency
9.	Exploitation of weaknesses, ambiguities and gaps in legislation	**22.**	Military exercises *
10.	Paramilitary groups	**23.**	Violation of airspace *
11.	Funding for religious and cultural groups	**24.**	Conventional/non-conventional force operations *
12.	Influencing curriculum and academia	**25.**	Intelligence / covert operations and infiltration *
13.	Promoting and exploiting corruption		

* due to the sensitive nature of these instruments, they have not been elaborated in separate chapters of the public version

Methodology

The methodology developed by the Centre for Countering Hybrid Threats specifically for this analysis is based on the aforementioned conceptual framework and model of the EU's Joint Research Centre (JRC), as well as other risk and vulnerability analysis techniques. An abbreviated version of it is presented in this chapter.

The analysis focused on 4 main areas:

- legislation and internal legislative measures,
- institutional structure and internal relations,
- the process of transferring and sharing information within and between entities and
- decision-making processes and the inputs involved.

It is important to stress that this is an analysis of the systemic set-up of the state administration and not an analysis of the operational and information content of the processes mentioned. Within this approach, the analysis was based on individual hybrid threats that are relevant to the national security and interests of the Slovak Republic. These hybrid threats can exploit specific vulnerabilities existing in government that, when combined with the potential impact of these threats, lead to risk.

Risk can also be treated or reduced by removing specific vulnerabilities, in the context of a scheme:

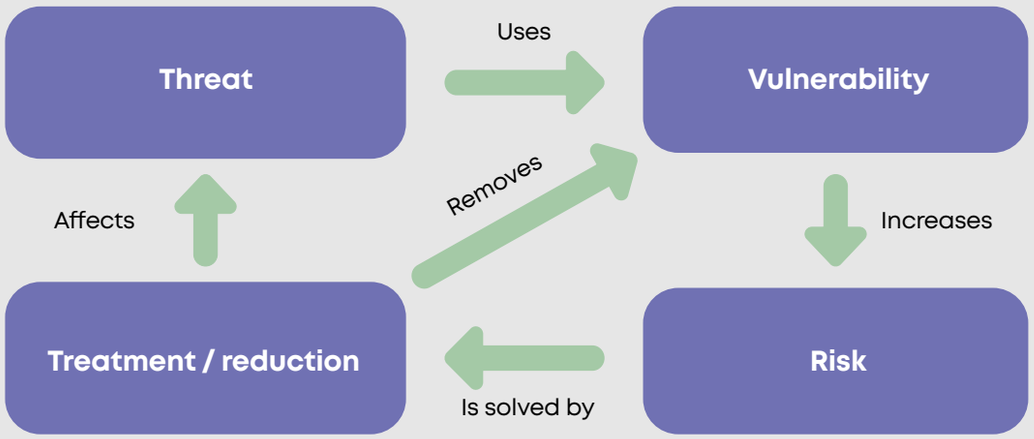


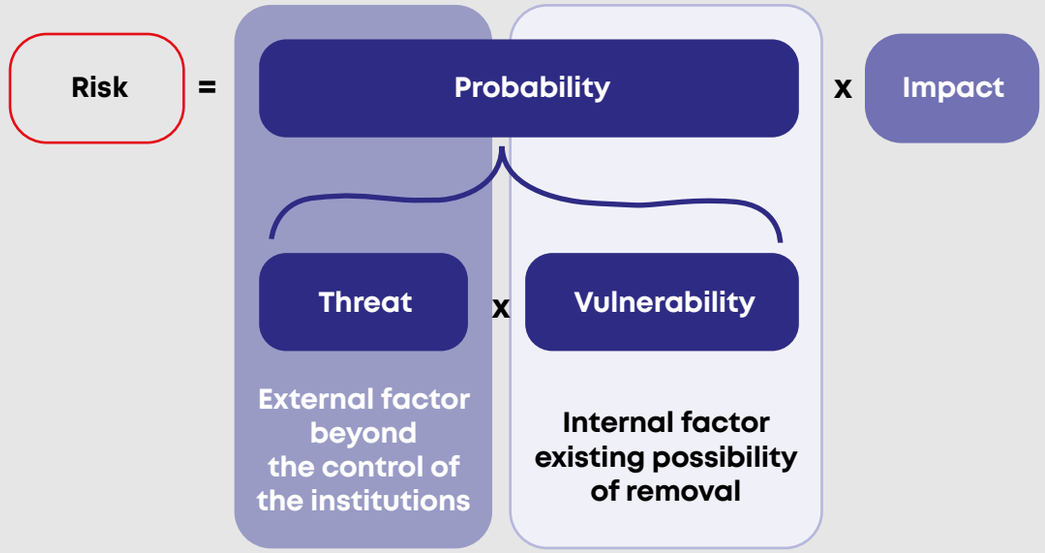
Figure 1 : Representation of the relationships between threat, vulnerability and risk[1]

[1] Inspired by Figure 1. of Toosarvandani, Marzieh & Modiri, Nasser & Afzali, Mehdi. (2012). The risk assessment and treatment approach in order to provide lan security based on isms standard. 10.5121/ijfcst.2012.2602

Each threat was assigned a lead authority - i.e. the institution with the greatest responsibility in the area - which was responsible for drafting a chapter on that threat in cooperation with the other institutions involved. In cooperation with the Centre for Countering Hybrid Threats, the task of authorities was to identify a list of processes that may be affected by hybrid threat instruments and to define a hypothetical scenario of how these processes could be exploited. Subsequently, the authorities proceeded on the basis of the reflective model "What? So what? Now what?" in three phases:

1. a description of the current state in terms of 4 main areas,
2. assessment of the current state and vulnerability analysis of the identified processes; and
3. proposal of measures to address identified vulnerabilities + their prioritisation on the basis of a qualitative risk analysis.

The qualitative risk analysis of the risk associated with the hybrid threat was carried out based on an assessment framework in which risk was expressed as the intersection of the respective value of the probability of the risk scenario being realised and the value of the level of potential impacts:



Figure[2] : Expressing risk as the intersection of probability and impact

[2] Inspired by Koen van Impe (2017) Simplifying Risk Management.
Available at: https://securityintelligence.com/simplifying-risk-management/

Authorities determined the resulting risk - extremely severe (A), high (B), low (C), or negligible (D) - as a combination of the likelihood of the risk scenario occurring and the "worst-case" possible impact, using definitions of each likelihood and impact level from the Center for Countering Hybrid Threats.

Likelihood of threat	Impact of the threat				
	Negligible	Minimum	Medium	Serious	Catastrophic
High	D	C	B	B	A
Medium	D	C	C	B	A
Low	D	D	D	C	B
Very low	D	D	D	D	C

Table 1: Determination of the level of resulting risk

The chapters, as well as the proposals for individual measures, have been finally prioritised according to the resulting level of risk and are marked with the corresponding colour.

System for countering hybrid threats

The broad possibilities of using hybrid instruments against the Slovak Republic lead to the need for increased coordination of activities within the state administration, as well as increased personnel capacity and sustainability of individual units dedicated to countering hybrid threats.

The system for countering hybrid threats must include:

- An efficiently set-up architecture of the institutions involved, including the division of their responsibilities
- Functional processes for coordination and information exchange between the institutions involved, to ensure practical measures to mitigate the impact of hybrid action
- A long-term strategy for the SK that will ensure the sustainability of the above institutional architecture and coordination processes.

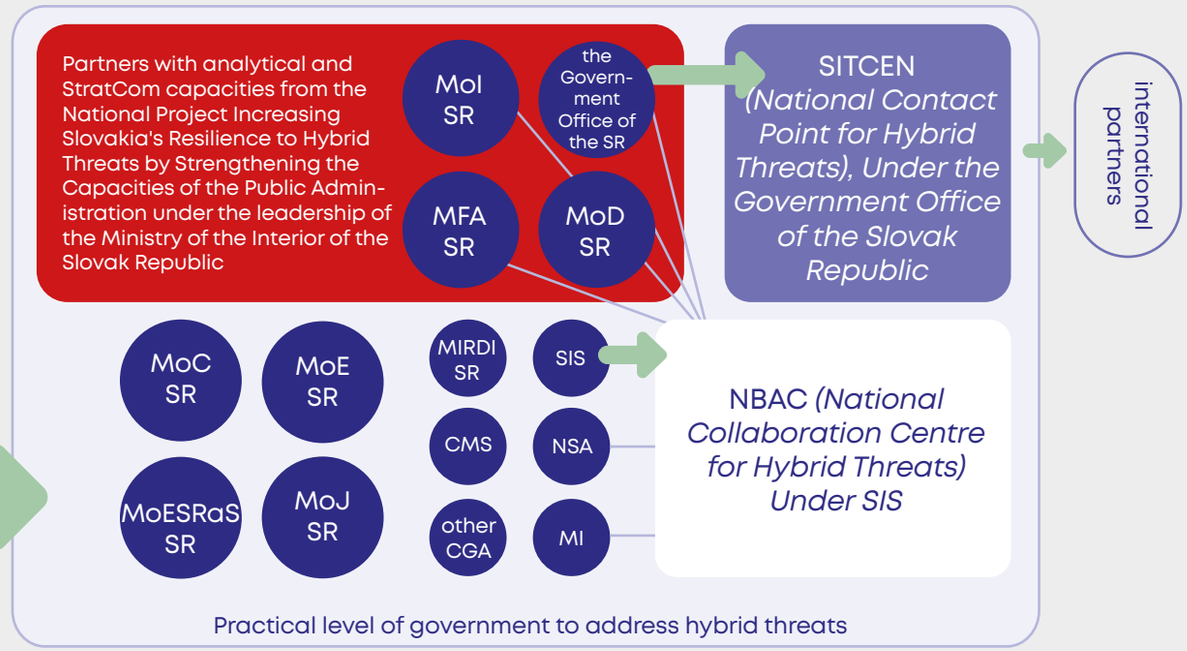
Non-implementation of measures to ensure coordination and sustainability of the expert components of the state administration dealing with hybrid threats poses a high risk of stagnation or even reduction of Slovakia's resilience to hybrid threats

Security Council Committee of the SK on Hybrid Threats

(strategic level of inter-ministerial cooperation)

Vulnerabilities identified	What needs to be done?
Lack of legislative anchoring of competences and designation of primary responsibility for countering hybrid threats	*Establish competencies and designate primary responsibility for coordinating the fight against hybrid threats in individual domains within state institutions*
Unsustainability of existing expert units and insufficient involvement of state institutions, which do not have specialised capacities to deal with hybrid threats	*Ensure the sustainability of the expert units established for strategic communication and countering hybrid threats and build capacity within state institutions where needed*
Lack of coordination between institutions dealing with hybrid threats	*Establish a central coordination mechanism or platform for the practical and operational coordination of services to counter hybrid threats*

Institutions dealing with hybrid threats



Disinformation campaigns and propaganda

Disinformation is the most commonly used instrument of hybrid threats. Hybrid actors can use them to influence public opinion, undermine trust in institutions, destabilise the political system or provoke unrest. Their objective is to manipulate perceptions of reality and influence people's decision-making.

Forms of possible hybrid action

- spread of false or manipulative information in order to harm, gain an advantage or influence the target audience,
- spread conflicting narratives or conspiracy theories to create information chaos or reduce trust,
- deliberate information in favour of a hybrid actor,
- spread of disinformation through fake accounts or bots, targeted discrediting of individuals or population groups in the interest of a hybrid actor.

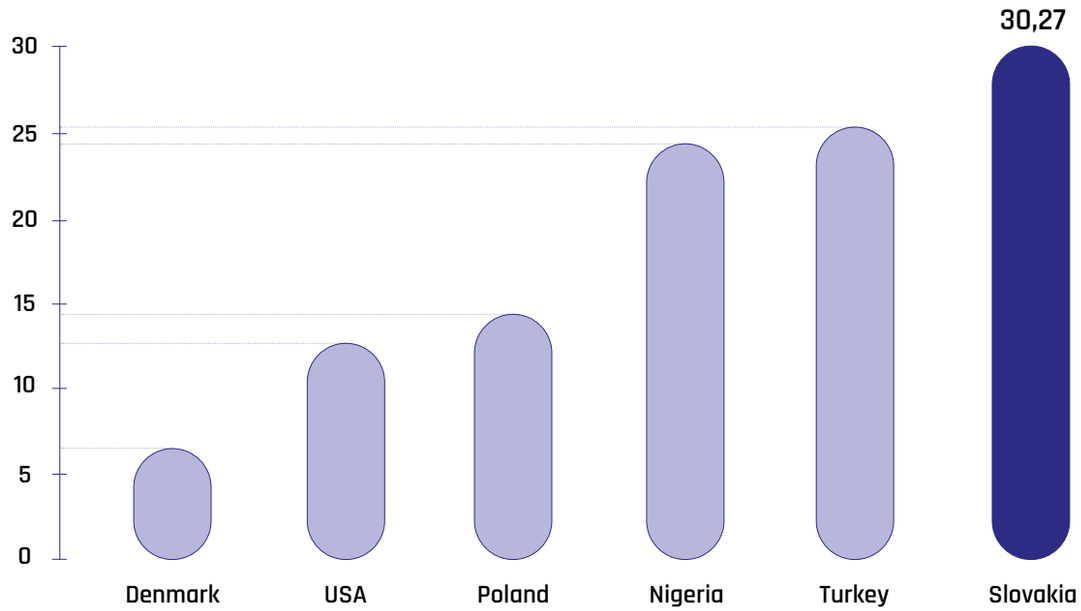
Intensive and long-term disinformation campaigns and propaganda cause polarisation of society, disruption of consensus on the foreign policy orientation of the Slovak Republic, reduction of trust in democratic institutions, as well as undermining or paralysing decision-making processes.

Institutions responsible

- Government Office of the Slovak Republic,
- Ministry of Interior of the Slovak Republic,
- Ministry of Foreign and European Affairs of the Slovak Republic.

Conspiracy Index

The so-called conspiracy index is calculated as the average of the positive answers to standard conspiracy questions. It is extremely high in Slovakia compared to the world.



Source: https://fmk.sk/konspiracny-index-na-slovensku/
Slovaks believe in conspiracies the most, UCM survey shows. In fmk.sk [online].

Vulnerabilities identified

Inability to block sites with a link to a hybrid actor.

Informality in the transfer and sharing of information between actors with an agenda in the fight against disinformation.

What needs to be done?

Adopt an amending law on Cybersecurity that would allow this step in eligible cases.

Consider amending the Competence Act to designate the entity primarily responsible for coordinating the fight against disinformation.

Influencing elections

This is a major threat to the Slovak Republic in the long term. Influencing elections undermines not only the integrity of the process itself, but also the democratic structure of the state

Forms of possible hybrid action

- implicit support for specific political candidates or parties, circumventing campaign and party funding restrictions and rules,
- decreasing public confidence in the results of elections and in state institutions,
- misuse of the internet and social networks to polarise society.

Successfully influencing elections can reduce citizens' trust in democratic institutions and elections. Furthermore, it also calls into question the Euro-Atlantic orientation of the Slovak Republic, which brings serious security implications.

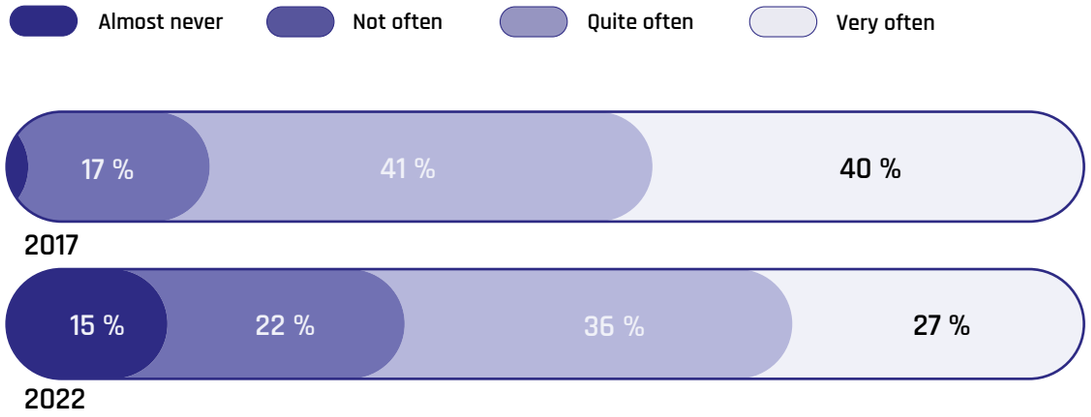
Institutions responsible

- Ministry of Interior of the Slovak Republic,
- State Commission for Elections and Control of Financing of Political Parties.

Confidence in Slovak elections

Comparison of 2017 with 2022

How often do you think votes are counted fairly in our country's elections?



Source: survey by Focus agency for Denník N

Source: https://dennikn.sk/minuta/2958750/

Vulnerabilities identified

What needs to be done?

The legislation indirectly allows the financing of political parties and election campaigns by foreign actors.	*Adopt more detailed legislation on the financing of political parties, movements and electoral campaigns in order to increase the transparency of electoral financing.*
Lack of explicit legal regulation of the electoral campaign before the referendum.	*Complete the legal regulation of the referendum election campaign.*
Legislation does not specifically reflect the conduct of electoral campaigns in the online space.	*Introduce legal regulation of online election campaigns. Plus define more precisely what constitutes an election campaign conducted on the internet (e.g. not only sponsored contributions).*

Weapons proliferation

There are several major arms companies in the Slovak Republic with production mainly abroad. These weapons go to war-torn countries or to countries that violate international embargoes. At the same time, so-called 80% weapons are found in the Slovak Republic and the problem of 3D weapons is growing.

Results of the arms amnesty in the Slovak Republic

(November 2020 - April 2021)

Returned

1 615 pcs
of illegally held weapons

53 025 pcs
illegally held ammunition

4th gun amnesty ended, Slovaks had over 1,600 firearms examined.

Press release of the Ministry of the Interior of the Slovak Republic of 06 May 2021

Source: https://www.minvsk.sk/tlacove-spravy/aspovat-sterilizacia-zbranova-amnestia

Forms of possible hybrid action

- illicit and licit trafficking in arms, ammunition, explosives, weapons components, explosives precursors and chemical warfare agents and dual-use items,
- proliferation of weapons through new technologies (so-called 3D weapons, which are difficult to detect without registration, and the so-called 80% of weapons not explicitly regulated),
- occurrence of a number of weapons and ammunition in illegal possession in the Slovak Republic.

Continuous proliferation of weapons can cause a serious threat to the security of the citizens of the Slovak Republic as well as the EU.

Institutions responsible

- Police Force,
- Financial Administration of the Slovak Republic,
- Ministry of Economy of the Slovak Republic.

Vulnerabilities identified

What needs to be done?

Lack of legislation in the area of 80% weapons and insufficient application of the legislation in force in relation to 3D weapons.	*Actively participate in the drafting of EU legislation on the so-called 80% weapons. Consistently apply the Slovak legislation on illegal arming with so-called 3D weapons.*
Lack of analysis and proactive monitoring of dual-use exports.	*Introduce a system of proactive analysis in the area of dual-use exports.*
Low analytical and technical capacity of the Police Force to counter illicit arms trafficking.	*Increase personnel and technical capacity to combat illicit arms trafficking.*

Cyber operations

Due to the widespread use of information systems, cyber-attacks are one of the most commonly used instruments of hybrid threats. Hybrid actors can undermine cybersecurity by penetrating networks and information systems.

Forms of possible hybrid action

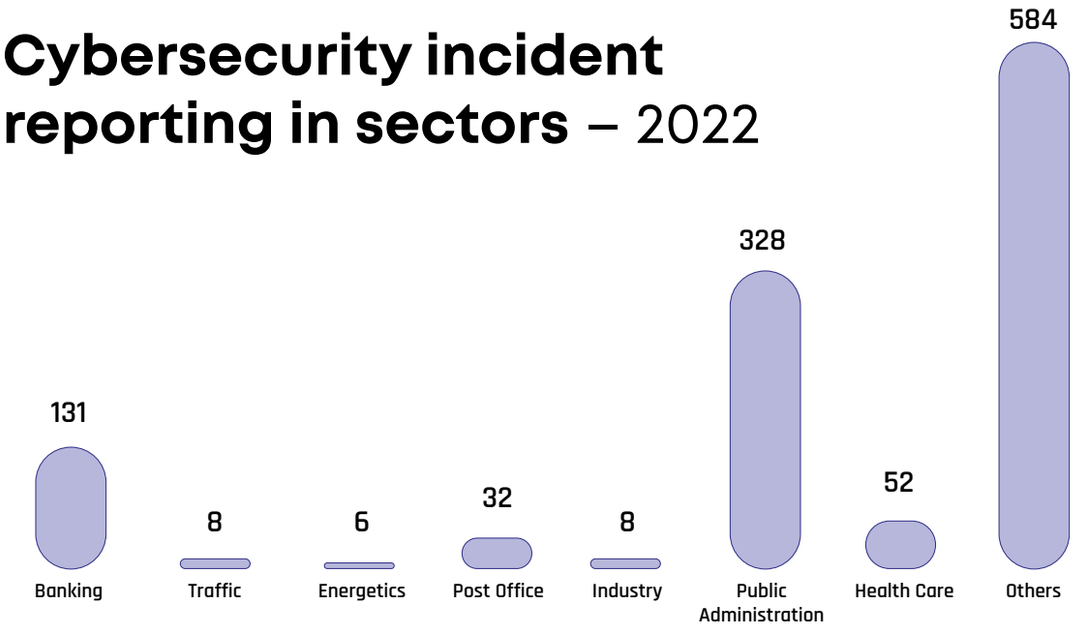
- complex cyber-attacks, if organised to take control of key systems or disable digital services,
- cyber espionage, whereby a hostile actor seeks to gain access to classified information, sensitive data, or intellectual property to gain advantage over a competing company or government entity.

A Cyber operations can have a catastrophic impact on the delivery of essential government services, the protection of the personal data of all citizens and public order.

Institutions responsible

- National Security Authority,
- central State administration bodies,
- operators of essential services,
- digital service providers.

Cybersecurity incident reporting in sectors – 2022



Source: https://www.nbu.gov.sk/wp-content/uploads/urad/Vyrocne_spravy/Sprava_Kyber_2022.pdf

Vulnerabilities identified

Failure to comply with the legal obligation to report every serious cyber security incident to the National Cyber Security Centre SK-CERT of the National Security Authority.

The cybersecurity risk analysis of some entities is often processed without a proper assessment of the operator's threats and vulnerabilities. Insufficient security measures are taken.

Ineffective methods of capacity building / undersized professional capacities in the field of cybersecurity.

What needs to be done?

Entities that are obliged to provide information under the Cybersecurity Act must immediately provide it free of charge and without delay.

Entities may follow the risk assessment methodology available on the website of the National Security Authority when analysing risks.

Ensure adequate professional capacity in the public administration.

Physical operations against infrastructure

Hybrid operations are often targeted against major infrastructure in the territory of the Slovak Republic and the EU. Hybrid actors can use different types of attacks to destabilise critical infrastructure (CI), the effects of which can be felt in different sectors.

Forms of possible hybrid action

- corruption,
- espionage,
- sabotage, cyber and physical attacks on critical systems and equipment,
- spread of misinformation and false information to destabilise the CI and cause chaos and insecurity,
- influencing key personnel at critical facilities or political leaders.

The most serious threat would occur when CI is disrupted. This would have adverse consequences for the state's ability to ensure the protection of life, health, safety, property or the environment.

Institutions responsible

- Government of the Slovak Republic,
- Ministry of Interior of the Slovak Republic.

CI sectors under the responsibility of central authorities

Source: https://www.zakonypreludi.sk/zz/2011-45
Act No. 45/2011 Coll., Act on Critical Infrastructure in zakonypreludi.sk [online].

Vulnerabilities identified

What needs to be done?

Vulnerabilities identified	What needs to be done?
Inadequacy of current legislation and strategies on CI.	*Amend the CI Act to reflect current security challenges and trends in this area.*
Outdatedness of the CI risk assessment.	*Adopt recommendations from the Action Plan for Coordinating the Fight against Hybrid Threats in the field of CI, incorporate hybrid threats into risk assessments, integrated crisis management and civil protection procedures and processes.*
Lack of experts to cover the CI protection agenda.	*Increase the capacity of CI and crisis management experts and analysts across the Central Governmental Authority, to ensure the long-term sustainability of these positions.*

Promoting social unrest and exploiting socio-cultural cleavages

In the socio-cultural sphere, hybrid actors focus on a wide range of topics, such as national identity, a country's history or religion, in order to create and deepen cleavages in society. Unemployment, poverty, migration and other issues that can cause social tensions can also be subject to abuse.

Forms of possible hybrid action

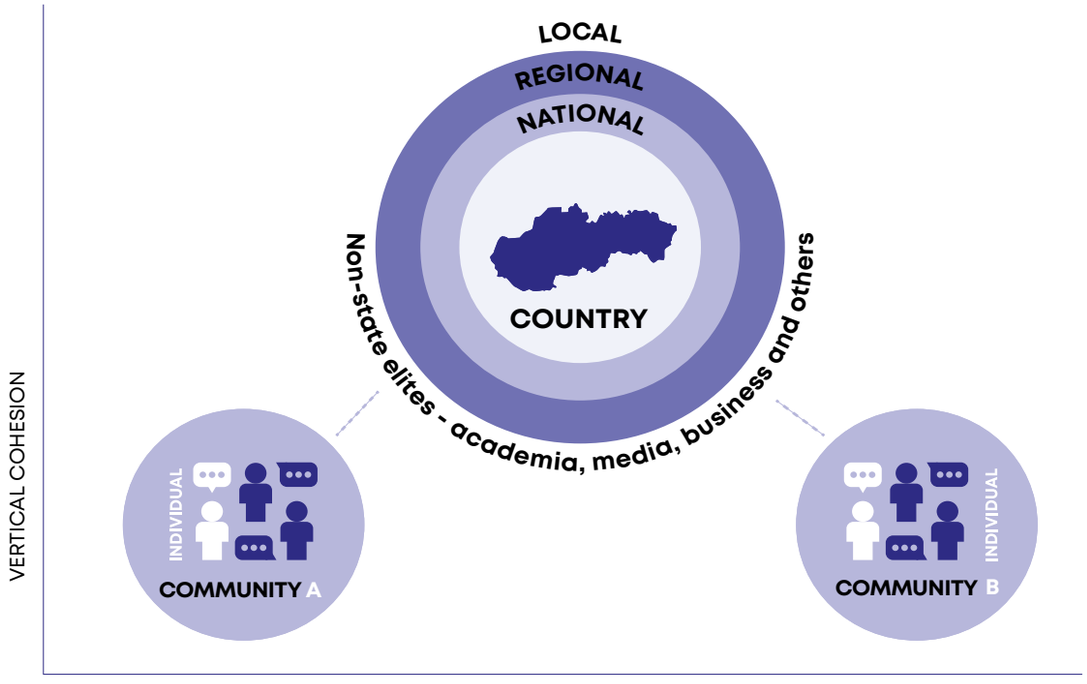
- Abuse of sensitive issues and their amplification through disinformation narratives to create tensions in society
- Exploitation of existing social cleavages to reinforce social tensions, polarisation or fear
- Promoting social unrest with the intention of influencing or disrupting the decision-making processes of the state

The hybrid actor seeks to change the foreign policy direction of the state or render its decision-making processes dysfunctional. This may undermine the performance of the basic functions of the state and reduce its ability to respond adequately in crisis situations.

Institutions responsible

Plenipotentiaries of the Government of the Slovak Republic - for the protection of freedom of religion or belief, for the development of civil society, for Roma communities and for national minorities.

Form of social cohesion in the state



Source: https://www.donio.sk/sudznost-na-slovensku

Vulnerabilities identified

Lack of principles and structures to ensure strategic governance in the Slovak Republic

No concept of building social cohesion

What needs to be done?

Institutionally anchor the principles of strategic governance to address complex societal problems beyond the length of electoral cycles.

Develop a concept for building social cohesion and resilience to the abuses of socio-cultural cleavages and the deliberate promotion of social unrest

Exploiting weaknesses in public administration

Weaknesses in the state administration are convenient targets for hybrid actors to weaken or influence the performance of the state administration. Weak protection and sharing of sensitive information, or lack of education and awareness of hybrid threats can be exploited

Forms of possible hybrid action

- influencing the opinion of public administration employees due to low awareness of hybrid threats and lack of education,
- abuse of the slow state response caused by complications associated with the transfer of classified information (personnel and technical),
- abuse of the lack of security technology on the part of the state, caused by the long procurement process.

In the event of a failure of the public administration, the responsiveness of the state and the trust of society in state institutions risk being undermined.

Institutions responsible

- Ministry of Interior of the Slovak Republic,
- all central State administration bodies.

Survey on hybrid threats in public administration (2018)

In your opinion, is your institution prepared to face hybrid threats?

Do you think you have sufficient knowledge of hybrid threat issues?

No Yes

(Source: Anonymous questionnaire survey of public administration employees in the framework of the project "Increasing preparedness and capacity of public administration for hybrid threats", GLOBSEC, November 2018)

Vulnerabilities identified

Lack of assessment of the reliability of applicants for public administration jobs in the online environment (e.g. social networks).

Lack of staff training on hybrid threats.

Lengthy and complicated procurement process for advanced security technologies.

What needs to be done?

Supplement the legislation on reliability assessment with activities in the online environment.

Introduce regular training for public administration employees on topics related to hybrid threats.

Accelerate the security procurement process.

Misuse of migration as a hybrid threat instrument

Hybrid actors can misuse or even deliberately induce a massive influx of foreigners into the Slovak Republic and the EU to polarise society. The consequence may be an increase in extremism and a disruption of society that the state may not be able to counter.

Forms of possible hybrid action

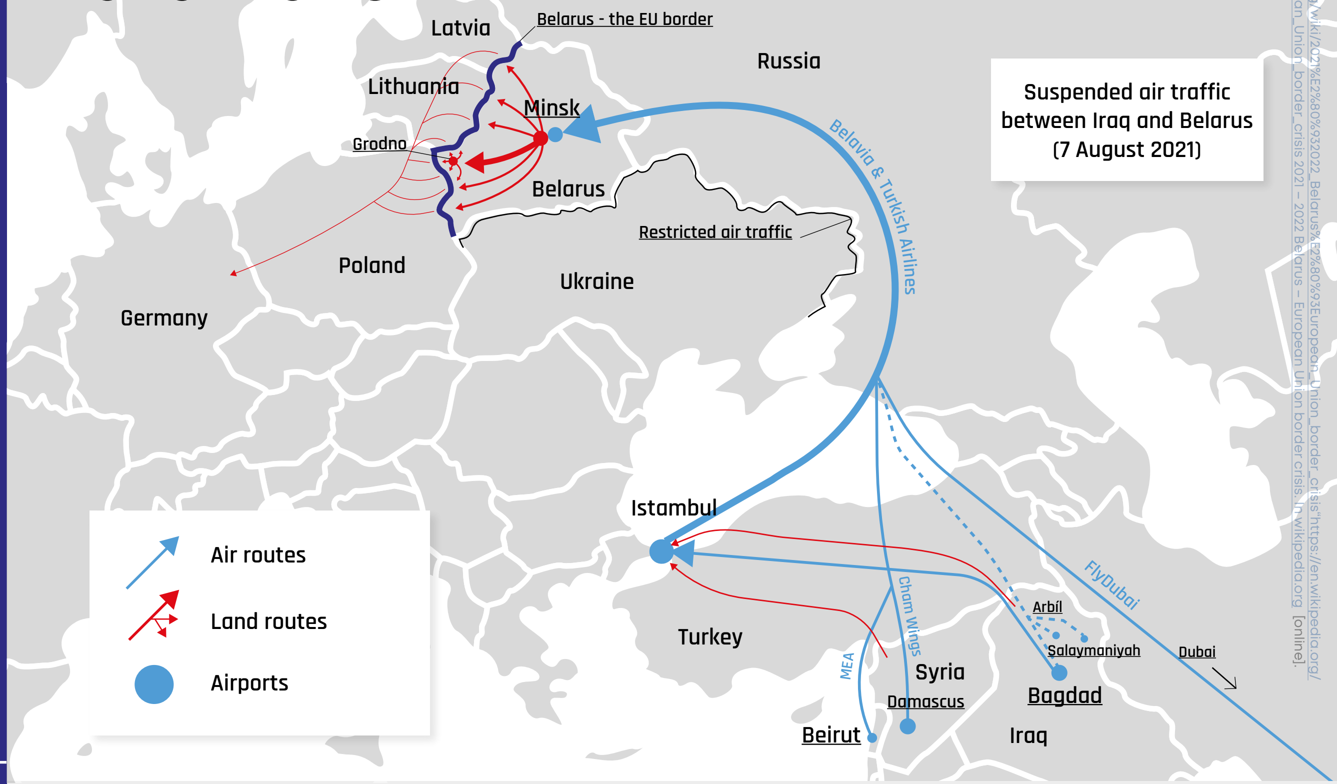
- organising and instigating irregular migration flows with the aim of instilling fear,
- attempts to reduce trust in state institutions and influence public opinion,
- polarisation of society, stirring up unrest and spreading misinformation about migrants.

In order to destabilize society, hybrid actors provoke conflicts and increase tensions between locals and foreigners. The border infrastructure is overloaded and the internal stability of both the Slovak Republic and the EU is weakened.

Institutions responsible

- Ministry of Interior of the Slovak Republic,
- Ministry of Foreign and European Affairs of the Slovak Republic.

2021-2022 artificially induced migration crisis on the border between Belarus and the EU



Source: https://en.wikipedia.org/wiki/2021%E2%80%932022_Belarus%E2%80%93European_Union_border_crisis"https://en.wikipedia.org/wiki/2021–2022_Belarus–European_Union_border_crisis 2021 – 2022 Belarus – European Union border crisis. In wikipedia.org [online].

Vulnerabilities identified		What needs to be done?
Irrelevance of the integration policy of the Slovak Republic.	➜	*Update the national strategy for the managed integration of returnees and migrants.*
Division of responsibilities for the migration agenda between several institutions.	➜	*Centralise the migration agenda in a single state institution.*
Inconsistency in the system structure of data collection and inter-ministerial data sharing.	➜	*Create a unified system of data collection structure to enable effective inter-ministerial data sharing and analysis.*

Exploitation of weaknesses, ambiguities and gaps in legislation

A hybrid actor can abuse against states their own law and democratic principles, as well as the process of law-making and its application against state interests.

Forms of possible hybrid action

- conducting non-legislative lobbying in support of the hybrid actor's strategic objectives,
- misuse of the Freedom of Information Act, leading to the disclosure of information to hybrid actors,
- influencing a Member or group of Members to bring forward and pass legislation expediently.

Attempts to influence the legislative process and the work of legislatures are common. In case of inappropriate or insufficient regulation of legislation, the enforcement of the interests of a hybrid actor may lead to the dysfunction of the security system of the Slovak Republic.

Institutions responsible

- Public administration bodies,
- Legislative Council of the Government of the Slovak Republic,
- Members or parliamentary groups.

Lobbying law not adopted for almost 2 decades

31 May 2005

Club 500: Act on lobbying should define in detail the forms of lobbyist's work

Bratislava, 31 May (Press agency of the Slovak Republic TASR) - Slovak businessmen associated in the Club 500 welcomed the draft Act on lobbying initiated by the Ministry of Justice,...

Press agency of the Slovak Republic **TASR**
Press Agency

Source: https://domov.sme.sk/c/2241431/klub-500-zakon-o-lobingu-by-mal-podrobne-vymedzit-formy-prace-lobistu.html
Club 500: The Lobbying Act should define in detail the forms of lobbying work. In sme.sk [online].

Vulnerabilities identified

Missing law on lobbying.

Unclear application rules of the Free Access to Information Act.

Lack of discussion in the abridged legislative procedure, where it is not possible to assess potential safety risks.

What needs to be done?

Adopt a law on lobbying, introduce rules on transparency of relations between constitutional officials and lobbyists.

Introduce a uniform methodology for the application of the law on free access to information.

Modify the legal conditions for the abridged legislative procedure, control of the use of this institute only in exceptional situations.

Paramilitary organisations

Paramilitary groups that are not integrated into the security forces of the state pose a significant security risk due to their influence and manipulation by hybrid actors. Indoctrination of their members with attitudes that are contrary to the national-state interests of the Slovak Republic can lead, especially during periods of destabilization of the security situation, to their misuse for physical operations or threats to security.

Forms of possible hybrid action

- armed and aggressive participation in riots,
- physical operations against the security forces of the Slovak Republic,
- intimidation of the population,
- conducting sabotage and physical attacks on critical systems and equipment,
- efforts to replace state forces,
- activities aimed at supporting domestic radical organisations.

The most serious threat would occur if a hybrid actor were to take complete control of such organisations. Their misuse would have serious implications for the state's ability to ensure the protection of the life, health, safety, and property of its own citizens.

Institutions responsible

- Ministry of Defence of the Slovak Republic,
- Ministry of the Interior of the Slovak Republic,
- intelligence services.

Activities of paramilitary organisations in the Slovak Republic

4 October 2015 06:55 pm

Slovak conscripts are trained by a professional soldier, the army is silent

MIRO KERN

The instructor of the paramilitary organization is a soldier from an anti-aircraft brigade who has received training from the Russian "military-patriotic" association. The conscripts are getting ready to attend school again.

Source: https://dennikn.sk/250730/slovenskych-brancov-cvici-profesionalny-vojak-armada-mici/ Slovenských brancov cvičí profesionálny vojak, armáda mlčí. In dennikn.sk [online].

Vulnerabilities identified

Low state control over existing paramilitary organisations.

Lack of legislation dealing with youth and young adults interested in defence activities.

Lack of an attractive and accessible alternative to paramilitary organisations.

What needs to be done?

Put in place mechanisms to ensure better control of paramilitary organisations by state institutions.

Introduce legislation to enable the development of conscription awareness and a healthy patriotism based on democratic values and centred on the military.

Create a state-accredited and regulated alternative to paramilitary organisations led by instructors who are current or former members of the armed forces or security forces.

Funding cultural groups or think tanks

Several states use culture and think tanks as a way to spread their power (e.g. China through the Confucius Institutes). Religious societies and secular organisations can also become instruments of hybrid action.

Forms of possible hybrid action

- provision of finance from abroad,
- involvement of members of churches and religious societies in illegal activities or armed conflicts outside the territory of the Slovak Republic,
- spreading misinformation or harmful information,
- making efforts to change the democratic establishment of the Slovak Republic.

A hybrid actor can use these groups to implement its strategic objectives. The result can be a long-term impact on public opinion, spreading extremism and influencing political developments in the country.

Institutions responsible

- Ministry of Culture of the Slovak Republic.

Communication of the Director of the Confucius Institute

22 April 2021 01:00 pm

Do you sleep well? You should be under a lot of stress. The head of a Chinese institute wrote to a Slovak expert

MIREK TÓDA

China is building influence in the academic world and trying to suppress free and critical debate about its regime, says Slovak researcher Matej Šimalčík, who was threatened by the head of the Confucius Institute in a threatening email.

Source: https://dennikn.sk/2367891/ef-cinskeho-institutu-pise-slovenskemu-expertovi/
Do you sleep well? You should be under a lot of stress. The head of a Chinese institute writes to a Slovak expert.In

Vulnerabilities identified	What needs to be done?
Insufficient overview of the activities of unregistered churches and insufficient communication with them.	*Extend the competences of the Ministry of Culture of the Slovak Republic and reconsider the process of registration of churches and religious societies.*
Insufficient staff capacity for analysis and low number of forensic experts in the field of religious and political extremism.	*Expand the capacity of the Ministry of Culture of the Slovak Republic to include experts on the issue of extremism.*
Lack of cooperation with intelligence services and lack of monitoring.	*Establish an inter-ministerial working group and strengthen institutional communication.*

Influencing curriculum and academics

Hybrid actors can exert long-term influence on the younger generation through the educational process, shaping their attitudes and promoting their own political, ideological or religious narratives contrary to the system of fundamental rights and freedoms and democratic values.

Forms of possible hybrid action

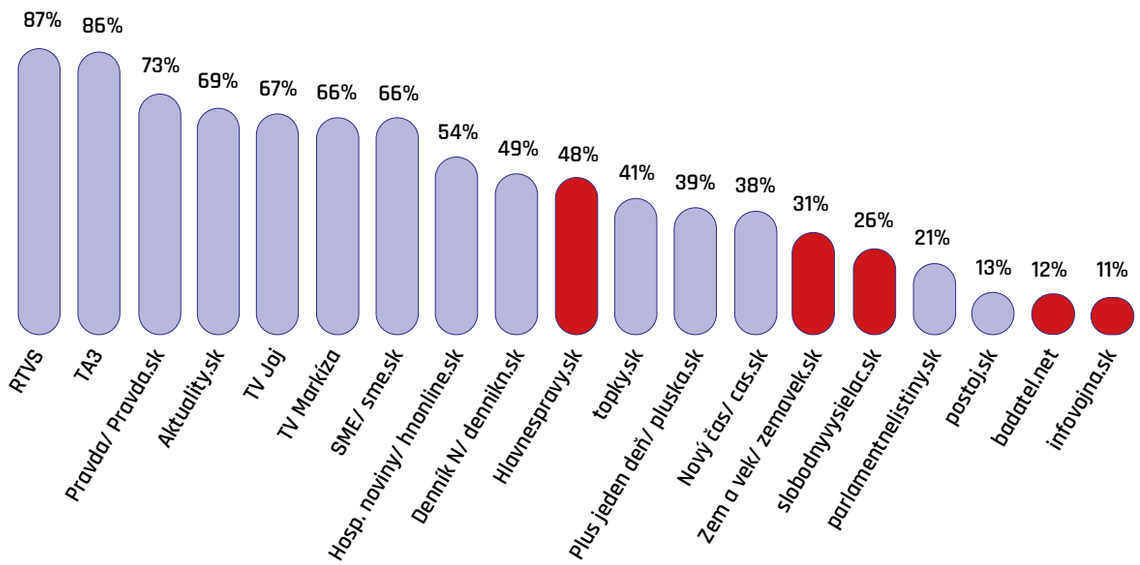
- influencing the curriculum - trying to manipulate its content by a hybrid actor,
- forging partnerships and building contacts in order to disseminate propaganda, influence critical thinking or advocate for personnel changes,
- obtaining information on research and development of critical innovations and technologies,
- putting pressure on employees of the Department of Education.

Such influence threatens the education system and academic freedom. This can manifest itself in reduced social cohesion and increased sympathy for the hybrid actor.

Institutions responsible

- Ministry of Education, Science, Research and Sport of the Slovak Republic,
- intelligence services.

Teacher survey on media credibility



Source: https://eduworld.sk/cd/rosi/776/prieskum-medzi-ucitelmi-ockovanie-je-pripravou-na-cipovanie-ludi

Note: the marked sites are identified as sites with questionable content by the konspiratori.sk project https://konspiratori.sk/zoznam-stranok

Vulnerabilities identified

Lack of professional capacities in the Department of Education that would specifically cover the issue of hybrid threats.

Low level of awareness of hybrid threats in the Department of Education.

What needs to be done?

To provide financial, personnel and material-technical support for the creation of professional capacities in the Department of Education and thus to increase the capacity to respond flexibly to the incentives received.

Prepare awareness-raising activities for the relevant circle of people, in order to develop awareness of hybrid threats in the Department of Education.

Exploiting strategic corruption

By encouraging and exploiting corruption, hybrid actors seek to gain political influence, manipulate public opinion or leak classified information. Corruption undermines trust in the rule of law and its institutions, and such a weakened state is an easier target for hybrid action.

Forms of possible hybrid action

- providing bribes to politically exposed persons to promote certain policies,
- trying to win the affection of politicians, the media or public figures through donations, invitations to social events or other benefits,
- building a network of affiliates to influence public opinion and question the fundamental institutions of the state,
- the use of persons who are recipients of classified information for cooperation and the disclosure of such information.

If the state does not act against the promotion and use of corruption, it jeopardises the functioning of fundamental institutions and undermines their decision-making mechanisms. Social and political stability can be undermined as a result.

Institutions responsible

- Government Office of the Slovak Republic,
- Ministry of Interior of the Slovak Republic,
- intelligence services.

Example of gaining influence through corruption

Qatar's Scandal: the European Parliament suspends the vice-president accused of corruption

Author: Barbara Zmušková and EURACTIV.com | EURACTIV.sk | Translation: Tatiana Turisová
13 Dec 2022 (updated: 14 Dec 2022)

The Greek Vice-President of the European Parliament, Eva Kaili, has been detained on suspicion of corruption after Belgian investigators found "bags full of money" at her home. The Conference of Presidents proposed to remove her from office and the European Parliament approved the proposal with a single vote against.

Four other suspects have been charged and arrested, including her partner Francesco Giorgi, who worked as an assistant to another MEP. Former MEP Pier Antonio Panzeri, in whose house a large amount of money was found, and Panzeri's former assistant were also charged.

Source: https://euractiv.sk/section/buducnost-eu/news/katarsky-skandal-europarlament-zbavil-funkcie-podpredsednicku-obvinenu-z-korupcie/

Vulnerabilities identified	What needs to be done?
Unsystematic classification of certain corruption offences within the breakdown of the Criminal Code.	*Review the provisions of the Criminal Code with a view to deleting, adding or transferring certain offences under the offence of corruption.*
Lack of comprehensive exchange of information between the Ministry of the Interior of the Slovak Republic and intelligence services.	*Adapt the activities of the Security Council Committee of the Slovak Republic on Intelligence Coordination to provide a platform for effective and regular exchange of information between the Ministry of the Interior of the Slovak Republic and the intelligence services*

Pressure on politicians or members of the government

Hybrid actors can use a wide range of means of pressure on politicians or state officials in ways that go beyond legitimate means of promoting interests (e.g. lobbying). Such pressure includes unlawful acts or threats of violence.

Forms of possible hybrid action

- threatening, blackmailing and coercive behaviour,
- disclosure of sensitive information to hybrid actors,
- doxxing - publishing personal information such as address, phone number, etc.,
- organised assemblies or protests with an element of violence,
- defamation and discrediting in public space using false information/visuals.

Hybrid actors primarily aim to influence, paralyse or undermine the decision-making processes of the state in order to achieve their interests. Coercion can be exerted by foreign hostile actors through organised criminal groups or even various legal entities.

Institutions responsible

- Ministry of Interior of the Slovak Republic,
- intelligence services.

Example of pressure on political leaders (2021)

A BLOODY MESSAGE TO THE ENTIRE GOVERNMENT OF THE SLOVAK REPUBLIC, PRESIDENT ČAPUTOVÁ, HENCHMEN AND TRAITORS

Ultimatum for the entire government to resign

You who call yourselves the Government of the Slovak Republic are called upon to resign by 31 March 2021. We will not negotiate with you! If you do not resign, cruel and bloody times await you. No one will help you, you have few people to protect you from us.

We have contacts with addresses (also temporary ones) for all of you, including your families, military officials and the entire police force. If you don't resign, we are ready to go into a bloody fight for freedom!

We will gradually begin to destroy government buildings and associated offices, later the objects of the security and defence forces of the state, followed by the complete fleet of the entire state apparatus. You don't have that many firefighting units to put everything out.

The Government Office will burn in flames!

You have imposed a regime of chaos here, now we will show you chaos.

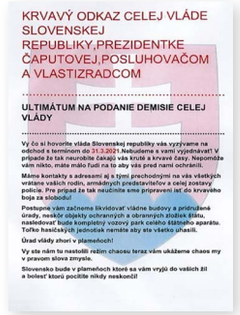
Slovakia will be in flames that will score into your veins and the pain you will feel will never end!

This will be followed by an attack on your SIS henchmen and all your confidants, including soldiers and policemen. Following that, their wives, their children, their parents! We will have no mercy on anyone.

Lives will be lost in the fight for freedom!

We will eliminate all informers, cowards and sell-outs! We will never allow our Slovakia to fall into someone else's hands, our country will rather burn to the ground than let that happen. You sellouts will burn up in the first place. We will take our country back! This bloody fight will not end until it is over. You will be held accountable for everything you have caused, everything you have stolen will be taken back from you.

Our Slovakia will remain ours and we are ready to put our lives on the line for that! We have nothing to lose. We will fight to our last breath.


KRVAVÝ ODKAZ CELEJ VLÁDE SLOVENSKEJ REPUBLIKY,PREZIDENTKE ČAPUTOVEJ,POSLUHOVAČOM A VLASTIZRADCOM

ULTIMÁTUM NA PODANIE DEMISIE CELEJ VLÁDY

Vy čo si hovoríte vláda Slovenskej republiky vás vyzývame na odchod s termínom do 31.3.2021.Nebudeme s vami vyjednávať! V prípade že tak neurobíte čakajú vás kruté a krvavé časy. Nepomôže vám nikto, máte málo ľudí na to aby vás pred nami ochránili.

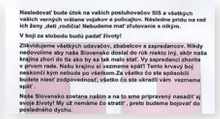
Máme kontakty s adresami aj s tými prechodnými na vás všetkých vrátane vašich rodín, armádnych predstaviteľov a celej zostavy polície. Pre prípad že tak neučiníte sme pripravení ísť do krvavého boja za slobodu!

Postupne vám začneme likvidovať vládne budovy a pridružené úrady, neskôr objekty ochranných a obranných zložiek štátu, následovať bude kompletný vozový park celého štátneho aparátu. Toľko hasičských jednotiek nemáte aby ste všetko uhasili.

Úrad vlády zhorí v plameňoch!

Vy ste nám tu nastolili režim chaosu teraz vám ukážeme chaos my v pravom slova zmysle.

Slovensko bude v plameňoch ktoré sa vám vryjú do vašich žíl a bolesť ktorú pocítite nikdy neskončí


Nasledovať bude útok na vašich posluhovačov SIS a všetkých vašich verných vrátane vojakov a policajtov. Následne prídu na rad ich ženy ,deti ,rodičia! Nebudeme mať zľutovanie s nikým.

V boji za slobodu budú padať životy!

Zlikvidujeme všetkých udavačov, zbabelcov a zapredancov. Nikdy nedovolíme aby naša Slovensko skončil do rúk niekto iný, skôr naša krajina zhorí do tla ako by sa tak malo stať. Vy zapredanci zhoríte v prvom rade. Našu krajinu si vezmeme späť! Tento krvavý boj neskončí kým nebude po všetkom.Za všetko čo ste spôsobili budete nielen zodpovednosť, všetko čo ste ukradli vám vezmeme späť.

Naše Slovensko zostane našim a na to sme pripravený nasadiť aj svoje životy! My už nemáme čo stratiť , preto budeme bojovať do posledného dychu.

Visual of threats sent to several state institutions in 2021

Vulnerabilities identified

Low awareness of Members of the National Assembly of the Slovak Republic and their assistants on the issue of pressure on politicians and possible solutions.

Criminal legislation does not allow for the effective clarification and sanctioning of such coercion if the person concerned does not feel threatened.

What needs to be done?

Create specialised training for the Members of the National Assembly of the Slovak Republic and their assistants.

Establish a working group to review the criminalisation of coercion of politicians and members of the government in the Criminal Code.

Embassies

Embassies can be misused to exert diplomatic pressure, also as local command, control and coordination centres for information and intelligence operations. They can also be used to disseminate propaganda and create a network of domestic actors supporting the hybrid actor's goals

Forms of possible hybrid action

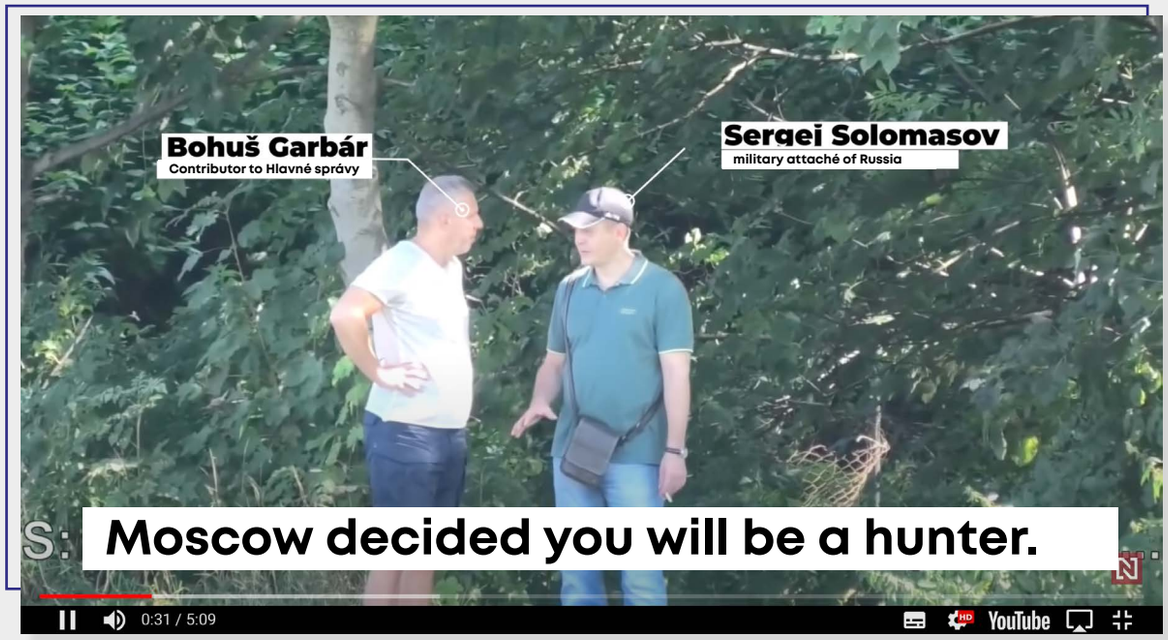
- posting of information services personnel under diplomatic cover,
- making contacts with government employees, attempts to obtain sensitive information,
- bribing disinformation and quasi-media in exchange for publishing articles that suit foreign policy interests,
- spreading misinformation through the embassy's official social media accounts.

In the Slovak Republic, activities of some countries misusing their embassies have been noted. The use of embassies for influence activities has the potential to influence public sentiment, destabilise the country and distort its foreign policy direction.

Institutions responsible

- Ministry of Foreign and European Affairs of the Slovak Republic,
- intelligence services.

Footage of Russian “diplomat" bribing the external contributor to Hlavné správy disinformation website



Source: https://dennikn.sk/2767779/ako-sa-verbuju-spioni-na-slovensku-povedal-som-v-moskve-ze-si-dobry-chlapec-video/

Leaked security footage shows a military attaché at the Russian embassy in Bratislava giving a bribe to a Hlavné správy (well known website spreading disinformation) contributor and recruiting him for espionage.

Source: Denník N

Vulnerabilities identified

Issuing consent for the arrival of diplomatic staff from other countries without thorough verification.

What needs to be done?

Introduce more effective control mechanisms to prevent misuse of diplomatic status by incoming foreign embassy staff.

Using diasporas for influence

Diasporas can become instruments of hybrid action when their activities are covertly manipulated by the government of a foreign state. The objective is to influence political processes, decision-making and public opinion in the host country in the long term.

Forms of possible hybrid action

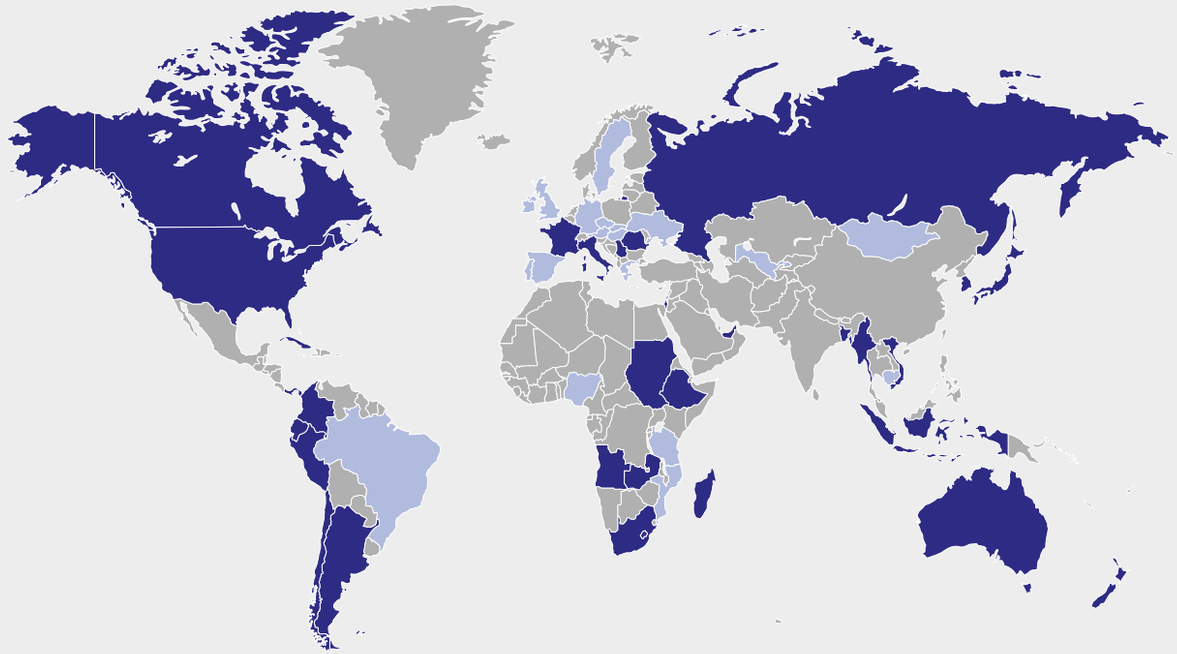
- funding of cultural institutes, associations or media and their misuse for activities glorifying the government of a foreign state,
- dissemination of a different perception of history and foreign policy among members of the diaspora,
- decreasing loyalty of diaspora members to the Slovak Republic,
- influencing the diaspora to support specific political actors,
- operation of agents within the diaspora under business cover and their participation in government contracts or the provision of technological equipment in sensitive areas

Compared to other EU states, there are currently relatively few diasporas in the Slovak Republic coming from countries that use hybrid action to achieve their goals.

Institutions responsible

- Ministry of Foreign and European Affairs of the Slovak Republic,
- Ministry of Culture of the Slovak Republic,
- Ministry of Education, Science, Research and Sport of the Slovak Republic.

The so-called Chinese police stations



Countries with known stations
Countries with newly discovered stations

Source: https://safeguarddefenders.com/en/blog/patrol-and-persuade-follow-110-overseas-investigation

In September 2022, the non-governmental human rights organisation Safeguard Defenders published a report exposing a network of so-called Chinese police stations operating in 53 countries around the world, including the Slovak Republic. These so-called police stations in some countries were reportedly involved in harassing, intimidating and coercing members of the Chinese diaspora abroad.

Vulnerabilities identified

Insufficient overview of the movement and use of funds spent on the activities of national minorities, ethnic groups and diasporas from abroad.

What needs to be done?

Introduce a monitoring system of financial flows to support diasporas from abroad.

Diplomatic and economic sanctions

Sanctions in the form of embargoes, tariffs and other measures can be used to weaken the economy, exert pressure and influence decision-making processes. At the same time, it is a legitimate instrument for democratic countries to protect their interests against hybrid actors

Forms of possible hybrid action

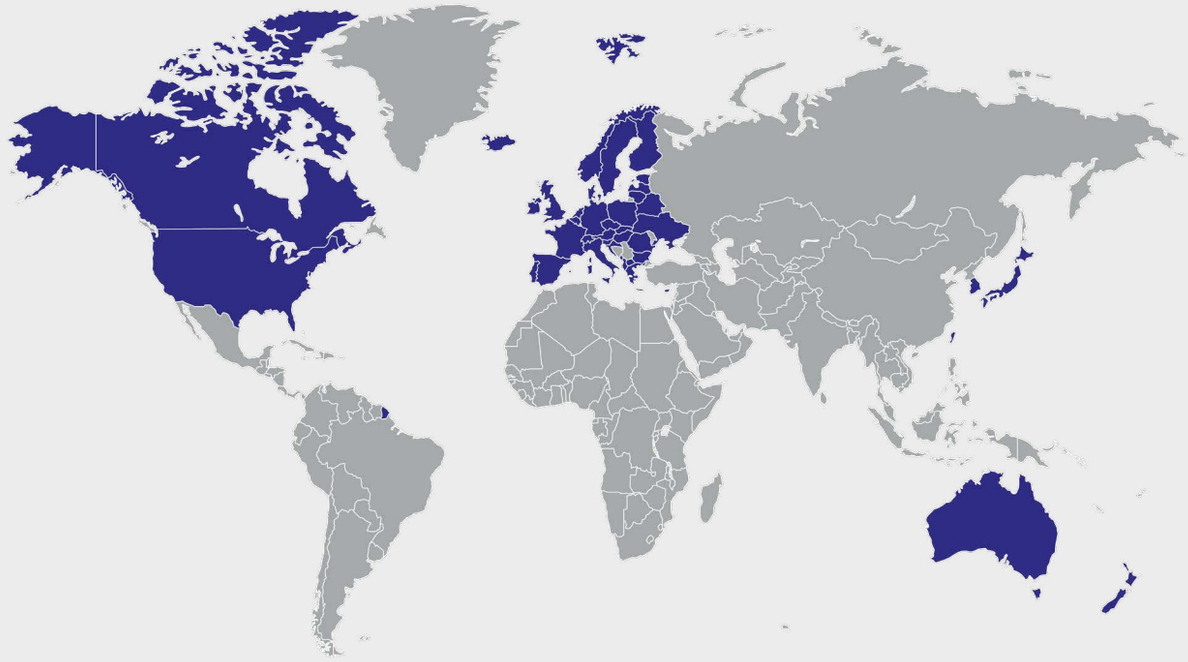
- travel bans as a form of coercion,
- severance or restriction of diplomatic ties,
- imposition of export restrictions,
- freezing the assets of selected companies in a foreign country.

The imposition of sanction is both symbolic and political and can have a significant impact on the mood of the society. The ability of the Slovak Republic and the EU to take retaliatory measures in an effective and timely manner significantly depends on the scope of hybrid actors.

Institutions responsible

- Government Office of the Slovak Republic,
- Ministry of Foreign and European Affairs of the Slovak Republic,
- Ministry of Economy of the Slovak Republic,
- Ministry of Finance of the Slovak Republic,
- Ministry of Justice of the Slovak Republic.

Russia's list of "hostile countries"



Source: http://government.ru/en/docs/46080/

In 2021, Russia published a list of "hostile countries" against which it imposed restrictive measures in response to their "hostile" behaviour. Since then, more countries have been added to the list (including Slovakia in 2022). Restrictive measures include visa restrictions, the obligation to pay for Russian gas in roubles, or limiting the number of local staff at embassies in Russia.

Source: official website of the Government of the Russian Federation

Vulnerabilities identified	What needs to be done?
Unclear definition of the competences of national authorities in the law on the implementation of international sanctions.	*Specify a legal regulation in the field of international sanctions that clearly establishes and determines the competences of the responsible ministries.*
Lack of practice in declaring national sanctions.	*Consider establishing a process for the adoption of national sanctions by the Slovak Republic and the subsequent establishment of the necessary staff capacity.*

Control and interference into the media

Media and media services can become an instrument of hybrid action. Hybrid actors seek to influence traditional media or to build a network of quasi-media and information channels on social networks in order to influence public opinion and destabilise society.

Forms of possible hybrid action

- controlling and interfering with the media, through political influence, infiltration, sponsorship of the media, or by gaining ownership control,
- spreading misinformation, harmful information and manipulative narratives through social networks and quasi-media,
- questioning credibility of traditional media.

Controlling and interfering in the media is a serious security risk that can threaten freedom of expression, public trust in public information and, ultimately, democracy itself.

Institutions responsible

- Council for Media Services,
- Ministry of Culture of the Slovak Republic.

Media and channel ecosystem under RF control

Media linked to Russian intelligence services

Media directly controlled by the Russian government

Vulnerabilities identified

Lack of implementing rules for the Media Services Act.

Lack of formalisation of cooperation between the Media Services Council and the intelligence and security services.

What needs to be done?

Adopt the missing implementing regulations resulting from the Media Services Act.

Formalise processes for cooperation between the regulator and security forces.

Source: Russia's Propaganda & Disinformation Ecosystem - 2022 Update & New Disclosures (substack.com)

Exchange of classified information

Public authorities also have an important role to play in effectively defending against intelligence operations and infiltrations, including their ability to seamlessly handle classified information at the necessary level.

Forms of possible hybrid action

- misuse of the inability of the public authorities concerned to keep informed of the nature and extent of emerging threats,
- the use of slow decision-making as an obstacle to the smooth exchange of classified information between public authorities.

Some public authorities do not have sufficient staff capacity with the relevant competences. As a consequence, they are not able to have access to classified information to the maximum extent and within a reasonable time.

Institutions responsible

- National Security Authority,
- Intelligence services,
- all central State administration bodies.

Informing citizens about Slovak Intelligence Service and Military intelligence activities

Source: https://www.sis.gov.sk/pre-vas/sprava-o-cinnosti.html
https://vs.mosr.sk/aktuality/

2.1.2 Hybrid threats and their forms of action

In the course of 2021, the SIS has seen an intensification of hybrid activities by the RF in the information, intelligence, social and cultural spheres. Activities in the cyber, economic and diplomatic spheres were carried out with unchanged intensity compared to the past. The objectives of the aforementioned activities were to influence political decision-making on strategic issues by creating social pressure, to systematically deepen contradictions in the internal social discourse, to disseminate propaganda and to penetrate the state apparatus with the intention of directing its activities in favour of the foreign policy priorities of the Russian Federation.

In the informational and social domains, the Russian Federation continued to promote pro-Kremlin narratives and to maintain the image of the importance of the Russian Federation for the preservation of peace and security in Europe and in the Russian Federation itself. The Russian Federation relied mainly on a historical narrative, which smoothly transitioned into a criticism of the EU and NATO attitudes and activities, and appealed to the historical, cultural and national affinity of the Slovak and Russian people.

The Embassy of the Russian Federation intensified its official online information activities aimed primarily at building a fa-
sian Federation in the subconscious
ortant aspect of media communica-
was the presentation of the Russian
in delivering the Sputnik V vaccine

and influential engagement with the
although the visibility and intensity
the public space decreased com-
interest has recently shifted from the
the field of science, technology
he risk of industrial espionage or
paganda into the most prestig-
the Slovak Republic.

Military Intelligence Activity Report 2021

Activities of foreign intelligence services
In the area of protection against foreign intelligence activities, military intelligence activities in 2021 focused on detection, intelligence documentation, analysis, and elimination of intelligence activities against the protected values and interests of the Slovak Republic. At the same time, knowledge about the activities of foreign intelligence services in countries where the development of the security situation may negatively affect the interests of the Slovak Republic was obtained.
The Slovak Republic has also been used by foreign intelligence services as a space for cross-border intelligence operations, when intelligence services of foreign powers carry out individual phases of their operations in several countries. In this context, military intelligence cooperates with partner services of NATO and EU Member States and conducts intelligence operations to eliminate the harmful influence of foreign intelligence services.

Russian Federation

Traditional intelligence procedures for recruiting active and former members of the Slovak Armed Forces, as well as persons with links to the defence ministry and regional and top politics of the Slovak Republic, continued to be used. Financial rewards
sian Federation remained the main
olishing cooperation. In 2021, Military
umber of successful operations that
Russian intelligence officers operat-
On the basis of the measures taken,
intelligence services of the Russian
in 2022 and the overall number of
of the Russian Federation on the ter-
will be significantly reduced.

Vulnerabilities identified

Insufficient staff capacity of public authorities to handle classified information above the classification level Restricted.

What needs to be done?

Ensure sufficient staff authorization to inspect classified information at a higher classification level in accordance with the objective needs of the authorities.

Foreign direct investment (FDI)

In addition to the overwhelmingly positive impact of inward FDI, there is currently a growing number of hostile investments made for the purpose of controlling infrastructure or acquiring know-how. Hybrid actors can use them to manipulate the investment environment and acquire strategic assets.

Forms of possible hybrid action

- gaining influence in a sector in order to disrupt it - e.g. health, finance, energy, defence, IT, media,
- gaining media coverage and subsequently influencing public opinion and spreading disinformation,
- gaining access to strategic raw materials or supplies with the intent to disrupt, damage, acquire or artificially affect their availability.

In the case of hostile FDI, third states may have access to sensitive technologies, know-how, critical infrastructure, supplies or services that are critical and strategic for the Slovak Republic. Such investments make it possible to gain influence in different sectors.

Institutions responsible

- Ministry of Economy of the Slovak Republic,
- Ministry of Foreign and European Affairs of the Slovak Republic,
- intelligence services.

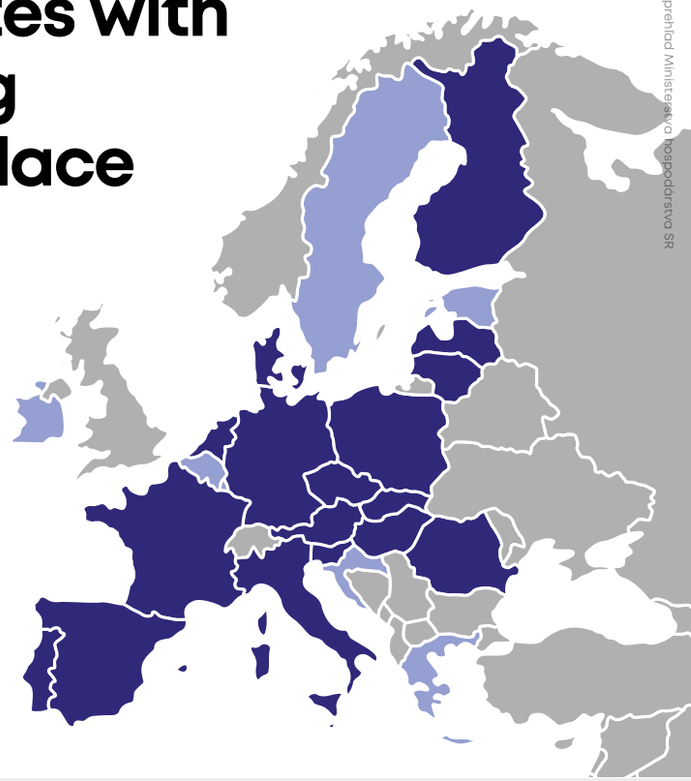
EU Member States with an FDI screening mechanism in place

Czech Republic, Denmark, Finland, France, the Netherlands, Lithuania, Latvia, Hungary, Malta, Germany, Poland, Portugal, Austria, Romania, Slovakia, Slovenia, Spain, Italy

EU Member States setting up an FDI screening mechanism

Belgium, Croatia, Estonia, Greece, Ireland, Luxembourg, Sweden

State as of 12 May 2023



Source: prehľad Ministerstva hospodárstva SR

Vulnerabilities identified

Lack of access to databases aggregating the necessary information on business entities.

Insufficient analytical capacity within the Ministry of Economy of the Slovak Republic.

Lack of certification of the application for sharing classified information between departments and intelligence services.

What needs to be done?

Purchase licenses for access to databases aggregating necessary information from all over the world on business entities and other persons that are part of a foreign investment.

Strengthen the staff capacity of the Ministry of Economy of the Slovak Republic for FDI screening.

Certify the application to share classified information at higher classification levels.

Creating and exploiting energy dependence

Dependence on the energy resources of other states allows hybrid actors to manipulate their prices, control infrastructure or threaten to cut off supplies if certain conditions are not met.

Forms of possible hybrid action

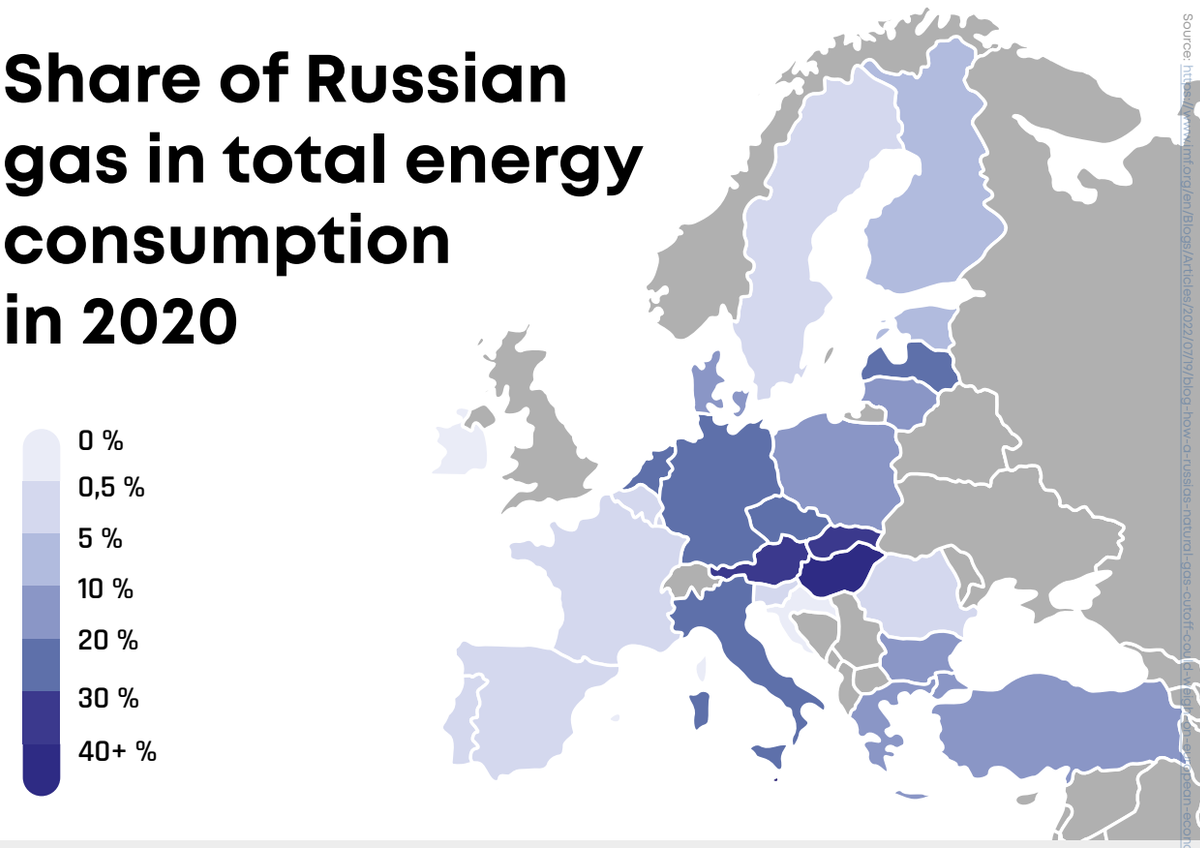
- manipulation of prices and availability of energy raw materials from outside the EU,
- cyber-attacks on energy infrastructure with the aim of disrupting the production or supply of electricity,
- influencing key infrastructure staff.

Energy dependence and price manipulation can affect the economy and lower the standard of living of the population. This can lead to polarisation of society, influencing the political situation and reducing trust in state institutions.

Institutions responsible

- Ministry of Economy of the Slovak Republic,
- Ministry of Foreign and European Affairs of the Slovak Republic,
- intelligence services.

Share of Russian gas in total energy consumption in 2020



Source: https://www.imf.org/en/Blogs/Articles/2022/07/19/blog-how-a-russias-natural-gas-cutoff-could-affect-europes-economies

Vulnerabilities identified

Slovakia's electricity sector risk preparedness plan out of date.

Outdated Integrated National Energy and Climate Plan.

Lack of a common data collection system for the energy sector.

What needs to be done?

Update the Slovak Republic's risk preparedness plan for the electricity sector.

Update the integrated national energy and climate plan in line with the requirements of Council and EP Regulation 2018/1999.

Support the creation of a common database in the energy sector at EU level in the framework of the REPowerEU reform.

Creating and exploiting economic hardship and dependency

Close economic ties can increase the strategic dependence of smaller countries on larger ones, binding them through sovereign debt or through unique or critical scarce commodities. The hybrid actors can disrupt supply chains and thus cause supply shortages of strategic raw materials.

Forms of possible hybrid action

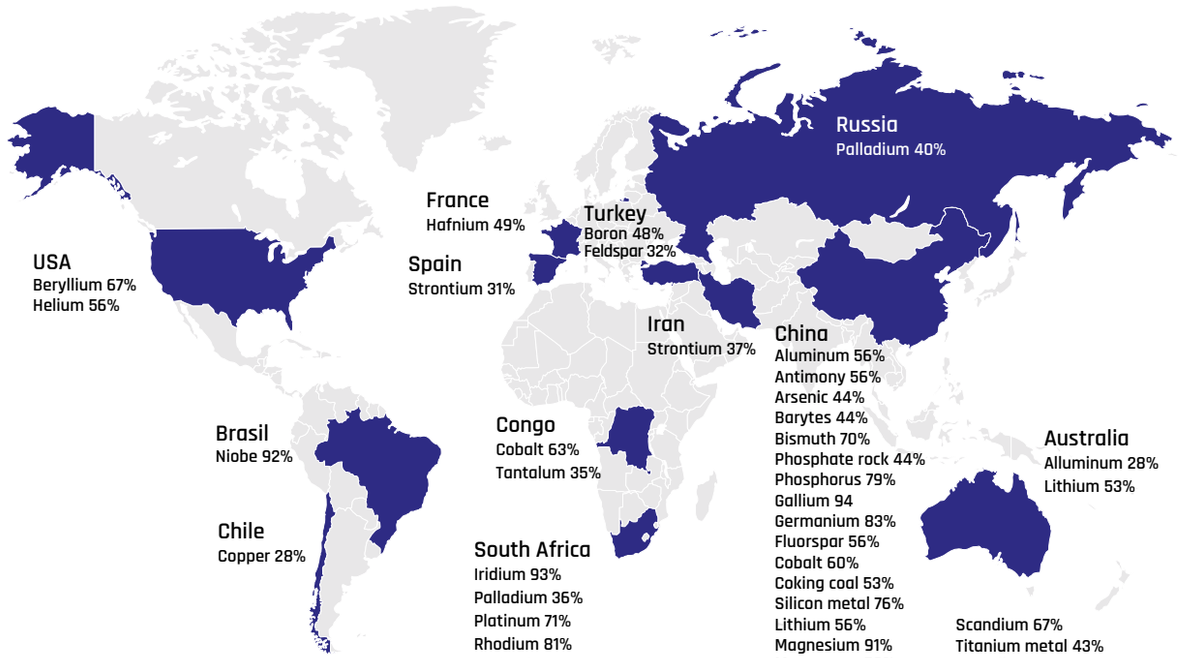
- building undiversified strategic partnerships for key commodities,
- exploiting country dependencies and favouring supply chains with related countries,
- influencing supply and artificially inflating the prices of critical raw materials and commodities.

Hybrid actors can exploit the slowdown in economic development and growth caused by a lack of competitiveness and the inability to secure financing from domestic markets. The aim is to question the legitimacy of the government and paint a picture of a failed state.

Institutions responsible

- Ministry of Economy of the Slovak Republic,
- Ministry of Foreign and European Affairs of the Slovak Republic.

Global distribution of critical minerals



Source: https://www.intereconomics.eu/contents/year/2023/number/2/article/the-eu-s-quest-for-strategic-raw-materials-what-role-for-recycling.html#:~:text=The%20CRM%20Act%20proposal%20sets,raw%20materials%20in%20the%20EU. The EU´s Quest for Strategic Raw Materials: What Role for Mining and Recycling? In intereconomics.eu [online].

Vulnerabilities identified

Unavailability of department-specific data on economic hardship and dependency.

Changes in EU initiatives and policies may have a direct impact on the difficulties and dependencies of Slovak industry.

What needs to be done?

Establish a system for sharing data on economic hardship and dependency among relevant government agencies.

Monitor the impact of EU policies and initiatives on Slovak industry and proactively communicate them with businesses and associations.

Conclusion

Thank you for your attention to this public analysis of vulnerabilities to hybrid threats. It is the result of a long-term effort and commitment to explore the new security challenges Slovakia faces in today's dynamically changing global landscape. We believe that collaboration with all stakeholders, including the public sector, the private sector and academic institutions, is essential to effectively address these threats.

We believe that this analysis will provide a basis for further building the Slovak Republic's resilience to hybrid threats. We have identified key areas where we need to increase our vigilance, prepare systemic changes related to legislative or institutional settings, or take practical preventive measures at the level of individual institutions. They aim to strengthen our country's defence capability and ensure preparedness for various possible scenarios.

We are aware that the tactics of hybrid actors, as well as the tools they use, are constantly changing, so it is critical to maintain expertise and update strategies and analytical outputs in this area on a regular basis. Together with our partners, we believe that we will be able to detect and respond quickly to potential threats.

However, this analysis is only the first step on a long journey to build a strong and resilient society. It will serve as a valuable foundation and compass as we develop new initiatives and policies to move us forward. During the preparation of this public version, our Centre for Countering Hybrid Threats of the Ministry of the Interior of the Slovak Republic started to prepare the Concept for Building Resilience of Public Administration against Hybrid Threats in the framework of Task C.1 of the Action Plan for Coordination of Countering Hybrid Threats, in order to translate the findings of the analysis into practice. In fact, the greatest added value of the analysis should lie in the implementation of the proposed actions that can move us step by step on our path to resilience.

In conclusion, we would like to once again express our deep gratitude to all those who have contributed to this analysis and to strengthening Slovakia's resilience to hybrid threats. Your commitment and dedication to a common goal are key to our shared success and security!

Glossary of terms and abbreviations

3D weapons – firearms, which are primarily produced using a 3D printer. According to Interpol, they can be categorised as fully 3D printed firearms, hybrid 3D printed firearms and firearms whose frame is produced in 3D printing.

80% weapons - an unfinished weapon, or a piece of metal that cannot be used as a firearm in its current form, but can easily be converted into one. The components are unregulated and readily available.

APHH – Action Plan for Countering Hybrid Threats Coordination, a document to strengthen state and societal resilience to hybrid threats.

Diaspora - a religious or ethnic community living (dispersed) within another (foreign) community.

Hybrid action - activities of state or non-state actors to undermine or damage a selected target using military and non-military methods (disinformation, propaganda, cyber-attacks…).

INEKP - Integrated National Energy and Climate Plan 2021-2030, addressing energy security, efficiency, competitiveness and sustainability, plus decarbonisation.

Lobbying - the process of influencing legislators, ministers and other public officials, or economic operators, by interest/pressure groups pursuing a common interest (called lobbies) in order to achieve a particular decision/action.

Migrant - a person who is outside the territory of his/her own country, residing in another country for more than one year, regardless of the reasons (voluntary, involuntary, war, economic) and the means of his/her migration to the country (regular or irregular).

Refugee - a person who has left home, most often because of fears of war; an applicant for temporary refuge in a foreign country.

Polarization (of society) - eradication, exacerbation with regard to contradictions, directing a grouping towards certain phenomena/realities.

Dual-use items - products or technologies developed for civilian purposes but in the wrong hands misused for human rights abuses or terrorist attacks (drones, chemicals).

Explosives precursors - chemicals that can be misused to construct homemade explosives (e.g. nitric acid, sulphuric acid, nitromethane…).

FDI - foreign direct investment in a foreign business enterprise for the purpose of acquiring a controlling interest in the enterprise (vertical, horizontal or conglomerate).

REPowerEU – reform to save and promote clean energy, diversify the EU's energy supply, and achieve a smart mix of investment and reform, with the aim of achieving at least a 55% reduction in net greenhouse gas emissions by 2030 and climate neutrality by 2050.

SK – Slovak Republic

PA - Public Administration, one of the forms of exercising public power

Think tanks – independent organisations that research and analyse public affairs issues. These include, for example, social policy, political strategy, economics, military affairs, technology, culture.

Central State administration bodies - this includes ministries and important offices (e.g. Government Office of the Slovak Republic, National Security Authority, etc.).

Public procurement - the rules and procedures for selecting a contractor, covering the award of contracts. Their aim is the efficient and economical use of public funds.

Basic bibliography for chapters

System for countering hybrid threats

- Concept of the Security System of the Slovak Republic
- Action Plan for the Coordination of Countering Hybrid Threats 2022-2024
- Security Strategy of the Slovak Republic
- Defence Strategy of the Slovak Republic
- Programme Declaration of the Government of the Slovak Republic 2023
- Programme Declaration of the Government of the Slovak Republic for the period 2021 - 2024

Disinformation campaigns and propaganda

- 1st EEAS Report on Foreign Information Manipulation and Interfe- rence Threats
- Council Conclusions on information manipulation and foreign interference (FIMI)
- Concept of Strategic Communication of the Slovak Republic
- Act No. 264/2022 Coll. on Media Services and on amendments and additions to certain acts
- Act No. 69/2018 Coll. on Cyber Security and on amendments to certain acts

Influencing elections

- Act No. 85/2005 Coll. on Political Parties and Political Movements, as amended
- Act No. 180/2014 Coll. on the Conditions for the exercise of voting rights
- Act No. 181/2014 Coll. on Election Campaign and on Amendment and Supplementation of Act No. 85/2005 Coll. on Political Parties and Political Movements, as amended
- Act No. 395/2022 Coll. on a special method of voting in a referendum announced on the basis of a citizens' petition adopted on 24 August 2022

Weapons proliferation

- Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 establishing a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items.
- Act No. 190/2003 Coll. of Laws on Firearms and Ammunition, and Amending Certain Acts
- Act No. 39/2011 Coll. of Laws on dual-use items and on amendments to Act No. 145/1995 Coll. of the National Council of the Slovak Republic on administrative fees and charges as amended

Cyber operations

- National Cybersecurity Strategy 2021-2025
- Action Plan for the Implementation of the National Cybersecurity Strategy 2021-2025
- Act No. 69/2018 Coll. on Cybersecurity and on amendments to certain laws
- Act No. 95/2019 Coll. on Information Technologies in the Public Administration

Physical operations against infrastructure

- Concept of Critical Infrastructure in the Slovak Republic and the method of its protection and defence approved by Government Res-olution No. 120 of 2007
- National Programme for the Protection and Defence of Critical Infra-structure in the Slovak Republic approved by Government Resolution No. 185/2008
- Act No. 45/2011 Coll. on Critical Infrastructure

Promoting social unrest and exploiting socio-cultural cleavages

- Concept of Social Inclusion of the Bratislava Self-Governing Region for 2020-2030
- Programme Slovakia 2021-27
- Strategy of equality, inclusion and participation of Roma until 2030
- Vision and strategy for Slovakia's development until 2030

Exploiting weaknesses in public administration

- Act No. 55/2017 Coll. on the Civil Service and amending certain acts
- Act No. 73/1998 Coll. on Civil Service of the Police Force member, Slovak Information Service, Corps of Prison Wardens and Judiciary guards of the Slovak Republic and Railway Police as subsequently amended,
- Act No. 315/2001 Coll. on Fire and Rescue Service as amended
- Act No. 215/2004 Coll. on the Protection of Classified Information

Misuse of migration as a hybrid threat instrument

- Integration Policy of the Slovak Republic 2014
- Contingency Plan of the Slovak Republic for dealing with the emergency situation in connection with the mass influx of the population of Ukraine to the territory of the Slovak Republic caused by the escalation of the armed conflict on the territory of Ukraine for the period October 2022 - March 2023
- Regulation (EU) 2019/1896 of the European Parliament and of the Council of 13 November 2019 on the European Border and Coast Guard and repealing Regulations (EU) No 1052/2013 and (EU) 2016/1624
- Act No. 480/2002 Coll. on Asylum and Amendments of Some Acts

Exploitation of weaknesses, ambiguities and gaps in legislation

- Act of the National Council of the Slovak Republic No. 350/1996 Coll. on Rules of Procedure of the National Council of the Slovak Republic, as amended
- Act No. 211/2000 Coll. on Free Access to Information and on amendments and supplement to certain acts
- Act No. 400/2015 Coll. on the Creation of Legal Regulations and on the Collection of Laws of the Slovak Republic and on the amendment and supplementation of certain laws as amended and by which certain laws are amended and supplemented

Paramilitary organisations

- Act No. 300/2005 Coll. on Criminal Code, as amended
- Act No. 83/1990 Coll. on Association of Citizens
- Act No. 85/2005 Coll. on Political Parties and Political Movements
- GLOBSEC - Hybrid Threats in Slovakia, Paramilitary and Extremist Groups, Analysis of Legislation, Structures and Processes

Funding cultural groups or think tanks

- Act No. 308/1991 Coll. on Freedom of Religious Faith and the position of churches and religious societies, as amended
- Act No. 213/1997 Coll. on Non-Profit Organisations providing services of general benefit
- Act No. 370/2019 Coll. on Financial Support for the Activities of Churches and Religious Societies

Influencing curriculum and academia

- State education programme
- Act No. 131/2002 Coll. on Higher Education and on Changes nad Supplements to Some Laws
- Act No. 245/2008 Coll. on the system of primary and secondary schools (School Act) as amended

Exploiting strategic corruption

- United Nations Convention against Corruption (UNCAC)
- National Anti-Corruption Programme of the Slovak Republic
- Anti-Corruption Policy of the Slovak Republic for 2019 - 2023
- Act No. 300/2005 Coll. on Criminal Code, as amended

Pressure on politicians or members of the government

- LP/2020/541 Principles of ensuring personal safety of designated persons and protection of designated objects
- Act No. 372/1990 Coll. on offences
- Act No. 40/164 Coll. on Civil Code

Embassies

- Vienna Convention
- Act No. 151/2010 Coll. on Foreign Service

Using diasporas to influence

- European Charter for Regional and Minority Languages
- Framework Convention for the Protection of National Minorities
- Act No. 184/1999 Coll. on the use of national minority languages

Diplomatic and economic sanctions

- Act No. 289/2016 Coll. on the Implementation of International Sanctions
- Act No. 575/2001 Coll. on the Organization of the Activity of the Government

Controlling and interfering with the media

- European Media Freedom Act)
- Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on the single market for digital services and amending Directive 2000/31/EC (Digital Services Act)
- Directive (EU) 2018/1808 of the European Parliament and of the Council of 14 November 2018 amending Directive 2010/13/EU (OJ L 303, 28.11.2018) (Audiovisual Media Services Directive)
- Act No. 264/2022 Coll. on Media Services and on Amendments and additions to certain acts

Foreign direct investment (FDI)

- Regulation (EU) 2019/452 of the European Parliament and of the Council establishing a framework for screening foreign direct investment into the Union
- Act No. 497/2022 Coll. on Screening of Foreign Direct Investments („FDI Act“)

Creating and exploiting energy dependence

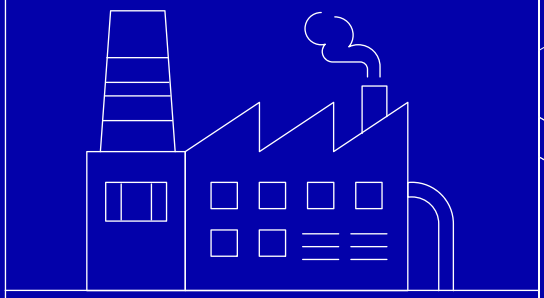
- Energy policy of the Slovak Republic
- INEKP - Integrated National Energy and Climate Plan 2021-2030
- Regulation (EU) 2017/1938 of the European Parliament and of the Council on measures to safeguard security of gas supply and repealing Regulation (EU) No 994/2010
- Act No. 251/2012 Coll. on Energy and on Amendments to Certain Acts

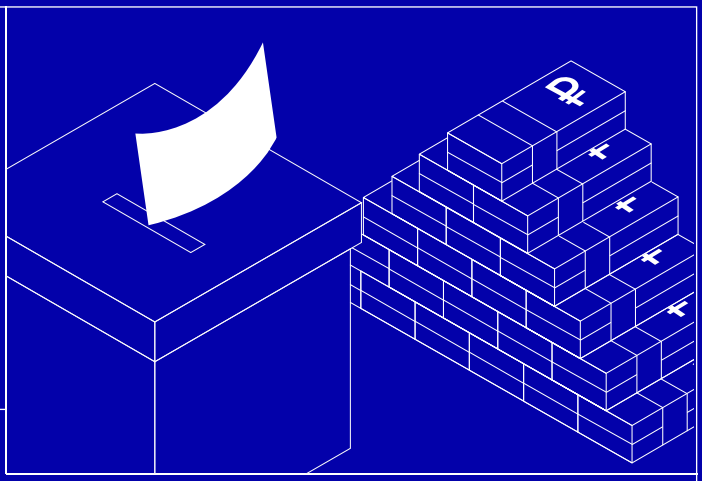
Creating and exploiting economic hardship and dependency

- Action plan 1 for the implementation of measures resulting from the Strategy of the Economic Policy of the Slovak Republic until 2030
- European Green Deal
- New EU industrial policy

Notes

Notes

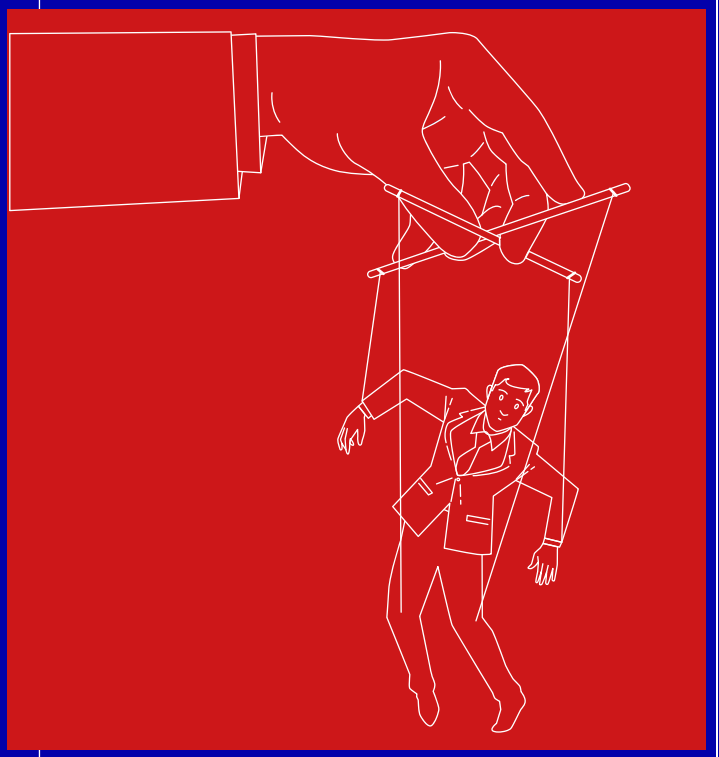


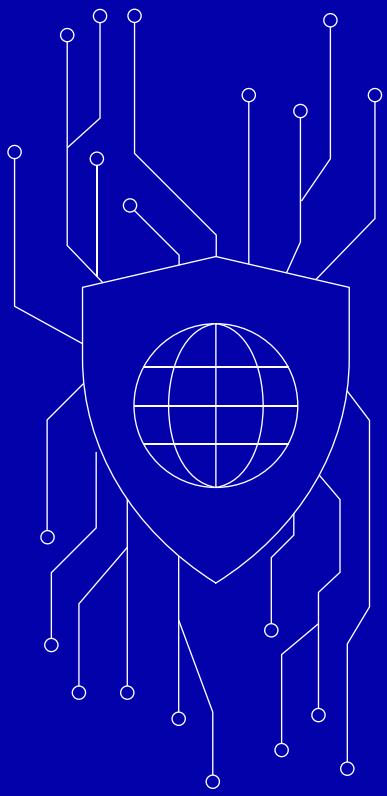


Centre for Countering Hybrid Threats (CBHH)

is an analytical, methodological and coordinating unit of the Slovak Ministry of the Interior in the field of hybrid threats. It operates within the Institute of Administrative and Security Analyses of the Ministry of Interior of the Slovak Republic since January 2022. The main objective of the Centre for Countering Hybrid Threats is to increase the capacity of the Ministry of the Interior of the Slovak Republic to monitor, analyse and counter various forms of hybrid threats. CBHH regularly collects data, analyses it, proposes measures and carries out activities in order to increase the resilience of public administrations to hybrid threats. The work focuses on 6 main areas:

- identification of key vulnerabilities to hybrid threats,
- implementing strategic communication based on data and analysis,
- streamlining public administration processes, structures and activities,
- raising the level of knowledge, competences and skills of public administration staff through training programmes,
- updating the regulatory framework and implementing data-driven public policy-making,
- increasing staff and technical capacity.





www.hybridnehrozby.sk | @CBHH_SK | hybrid@minv.sk